Análise Inteligente de Vulnerabilidades em Redes Locais Utilizando Inteligência Artificial

Maxwell Antonio, Isaías Rodrigues, Antony Isac, Lucas Evangelista
Orientadores: Credson isaac Lopes dos santos[1], Diego da Silva Pereira[2]

Resumo: O crescimento acelerado das tecnologias digitais e a expansão das redes de computadores aumentaram significativamente a superfície de ataque das organizações. A identificação rápida e precisa de vulnerabilidades é essencial para reduzir riscos e prevenir incidentes cibernéticos. Este trabalho propõe a utilização da Inteligência Artificial (IA) como mecanismo de análise inteligente em redes locais. A solução combina ferramentas como VirtualBox, Kali Linux, Ubuntu Server e Nmap, automatizando a coleta, organização e classificação de vulnerabilidades. Além disso, as informações são correlacionadas com bases oficiais como Common Vulnerabilities and Exposures (CVE) e National Vulnerability Database (NVD).

Palavras-chave: Inteligência Artificial; Cibersegurança; Redes Locais; Vulnerabilidades; Machine Learning; Nmap

INTRODUÇÃO

A transformação digital modificou profundamente a forma como empresas, instituições públicas e usuários utilizam sistemas computacionais. A crescente interconectividade entre dispositivos, servidores e serviços de rede trouxe inúmeros benefícios, mas também ampliou significativamente os riscos relacionados à segurança da informação. Segundo o relatório IBM Cost of a Data Breach Report 2024, o custo médio global de uma violação de dados atingiu novos máximos valores, evidenciando a necessidade de mecanismos cada vez mais eficientes para prevenção de ataques. Nesse contexto, a análise de vulnerabilidades representa uma das principais estratégias para identificar falhas que possam ser exploradas por agentes maliciosos. Ferramentas tradicionais de varredura, como o Nmap, são amplamente utilizadas para identificar portas abertas, serviços ativos, sistemas operacionais e possíveis configurações inseguras. Entretanto, a interpretação manual dos resultados pode tornar-se lenta e suscetível a erros, principalmente em redes com grande quantidade de dispositivos. A Inteligência Artificial surge como uma tecnologia capaz de complementar essas ferramentas por meio da análise automatizada de grandes volumes de dados, reconhecimento de padrões e classificação inteligente de riscos. Algoritmos de aprendizado de máquina podem identificar relações entre vulnerabilidades conhecidas, histórico de ataques e configurações de rede, permitindo priorizar automaticamente as falhas com maior potencial de exploração. Essa abordagem reduz o tempo gasto pelas equipes de segurança e aumenta a eficiência das ações preventivas. Dessa forma, este trabalho tem como objetivo apresentar uma proposta de integração entre técnicas de Inteligência Artificial e ferramentas de análise de vulnerabilidades em redes locais, demonstrando como essa combinação pode contribuir para fortalecer a segurança cibernética, otimizar processos de auditoria e apoiar a tomada de decisão baseada em evidências.

MATERIAL E MÉTODOS

A metodologia proposta neste trabalho tem como objetivo demonstrar a aplicação da Inteligência Artificial na automatização da análise de vulnerabilidades em uma rede local. Para isso, foi desenvolvido um ambiente virtualizado capaz de simular um cenário corporativo, permitindo a realização de testes de segurança sem comprometer equipamentos reais. O ambiente experimental foi construído utilizando o Oracle VM VirtualBox. Foram criadas duas máquinas virtuais principais: uma executando o Kali Linux, responsável pela realização das auditorias de segurança, e outra executando o Ubuntu Server, configurada como servidor alvo contendo serviços de rede e vulnerabilidades previamente definidas. A comunicação entre as máquinas foi realizada por meio de uma rede interna (Internal Network) denominada "labnet", impedindo que os testes afetassem outros dispositivos conectados à rede física.

Figura 1 – Configuração de rede da máquina Kali Linux. Esta imagem exibe a saída do comando `ip a` no terminal do Kali Linux, destacando o endereço IP 192.168.50.10 atribuído manualmente à interface de rede `eth1`.

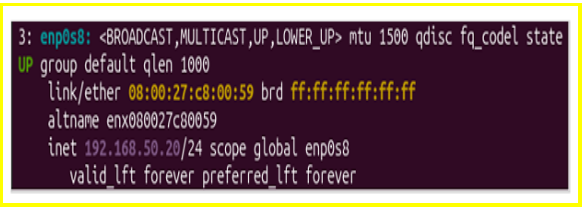

Figura 2 – Configuração de rede da máquina Ubuntu Server.

A captura mostra o endereço IP 192.168.50.20 configurado para a interface `enp0s8` do servidor alvo. Para a implementação do ambiente, os IPs foram configurados manualmente com o comando sudo ip addr add [ip]/24 dev [interface]. A conectividade foi validada por meio de testes de ping a partir do Kali Linux, confirmando que o host respondeu corretamente

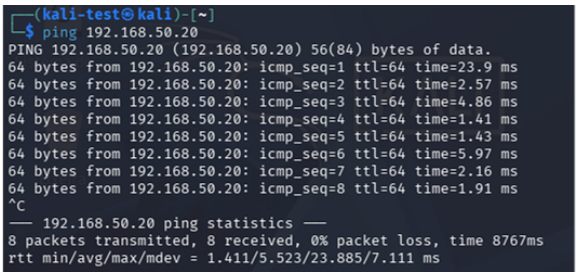

Figura 3 – Teste de conectividade (Ping).

A imagem apresenta a execução do comando `ping 192.168.50.20` a partir do Kali Linux, demonstrando uma troca de pacotes bem-sucedida com 0% de perda. Este teste é fundamental para validar que o canal de comunicação entre a ferramenta de análise e o alvo está ativo e funcional.

RESULTADOS E DISCUSSÃO

A análise prática demonstrou a eficácia da metodologia proposta no ambiente experimental. A varredura inicial de detecção de serviços, realizada com o comando nmap -sV 192.168.50.20, identificou o host como ativo, porém as 1000 portas analisadas apresentaram estado filtered (no-response)

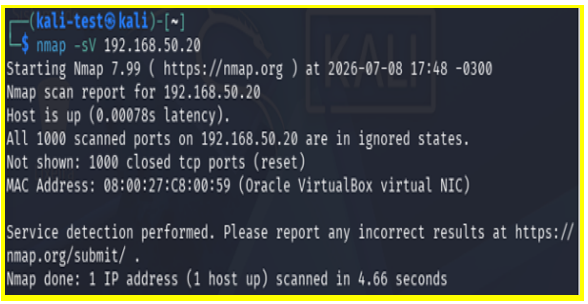

Figura 4 – Varredura inicial de serviços.

Esta imagem mostra a execução do comando `nmap -sV 192.168.50.20`. O resultado indica que o host está ativo, mas as portas estão filtradas, o que representa a primeira tentativa de descoberta de serviços expostos no alvo.

Para contornar a ausência de resposta inicial, foi executada uma nova varredura ignorando a descoberta padrão, utilizando o comando nmap -Pn -sV 192.168.50.20. O resultado confirmou o host ativo, mantendo as portas no estado filtered.

Figura 5 – Nova verificação ignorando descoberta inicial.

A captura exibe o uso do parâmetro ` Pn`, que força o Nmap a analisar as portas diretamente sem realizar a descoberta prévia por ping. O resultado de 1000 portas filtradas sugere a presença de mecanismos de defesa, como firewalls, protegendo o sistema Ubuntu.

A interpretação desses resultados indica que o sistema Ubuntu está acessível na rede, mas não apresenta serviços TCP expostos nas portas analisadas. O estado filtered sugere que as requisições enviadas pelo Nmap não receberam resposta, o que pode ser atribuído a um firewall bloqueando conexões externas, regras de filtragem de rede ou ausência de serviços ativos aguardando conexões. Nenhuma vulnerabilidade direta foi

identificada, como portas abertas, serviços desatualizados ou aplicações expostas. Foram observados pontos positivos de segurança, incluindo a ausência de serviços expostos desnecessários, a redução da superfície de ataque e a possível filtragem de conexões externas

CONCLUSÃO

Conclusão Este trabalho demonstrou a viabilidade e a eficácia da integração da Inteligência Artificial com ferramentas tradicionais de análise de vulnerabilidades em um ambiente de rede local simulado. A ferramenta Nmap foi essencial para a coleta técnica dos dados, enquanto a IA atuou como ferramenta de apoio fundamental na interpretação dos resultados, classificação de riscos e elaboração de medidas de mitigação

REFERÊNCIAS

IBM SECURITY. *Cost of a Data Breach Report 2024*. IBM Corporation, Armonk, 2024.

LYON, Gordon Fyodor. *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*. Insecure.Com LLC, Sunnyvale, 2009.

MITRE CORPORATION. *Common Vulnerabilities and Exposures (CVE)*. MITRE Corporation, McLean, 2024.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). *Cybersecurity Framework 2.0*. National Institute of Standards and Technology, Gaithersburg, 2024.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). *National Vulnerability Database (NVD)*. National Institute of Standards and Technology, Gaithersburg, 2024.

OFFENSIVE SECURITY. *Kali Linux Documentation*. Offensive Security, 2024.

ORACLE CORPORATION. *Oracle VM VirtualBox Documentation*. Oracle Corporation, Austin, 2024.

OWASP FOUNDATION. *OWASP Top 10: The Ten Most Critical Web Application Security Risks*. OWASP Foundation, Wakefield, 2021.