Title: Harnessing AI and Open-Source Tools for Enhanced IT Security Vulnerability Assessment

Presenter's Name and Affiliation: Joost Grunwald (SURF)

Presentation and Audience Description:
This presentation will be a comprehensive exploration of the research conducted on harnessing AI and open-source tools for enhanced IT security vulnerability assessment. The target audience for this presentation includes IT security professionals, vulnerability assessment specialists, and decision-makers in organizations seeking to optimize their IT security protocols and strategies.

Abstract:
In the ever-evolving landscape of IT security, the need to effectively identify and manage vulnerabilities is paramount. This study delves into how the amalgamation of different vulnerability scanners, coupled with open-source projects, can yield comprehensive and trustworthy data. It also elucidates how Artificial Intelligence (AI) plays a pivotal role in enriching reports and prioritizing vulnerabilities based on a multi-faceted equation of Threat, Risk, and assurance of an appropriate Tool.

Transitioning towards semi-automated penetration testing, the study delves into the utilization of AI in automatically verifying vulnerabilities as Proof of Concept (POC) exploits. Through the active confirmation of vulnerabilities using exploitation tools in conjunction with a Linux shell and a Metasploit console, the AI can assess multiple version-based vulnerabilities to validate their potential exploitability. This practice highlights the strength and effectiveness of integrating traditional vulnerability scanners with AI and open-source projects to bolster IT security.

Moreover, the study addresses the integration of cloud environments in the vulnerability assessment process. By scanning cloud environments for weaknesses, organizations can gain better insight into all publicly exposed parts of their infrastructure, leading to a more comprehensive understanding of their attack surface.

To cater to organizations with varying security requirements, the proposed solution offers modularity in tool selection. Organizations can choose from a range of scanning options, from internet-based scans (InternetDB, Shodan) that have minimal impact, to full vulnerability management and even penetration testing-like scans that attempt to exploit discovered vulnerabilities for validation.

The study showcases the innovative use of AI for generating solvability scores, which serve as a measure of how easy it is to fix a vulnerability. By mapping vulnerabilities to risk scores based on factors like EPSS, CVSS, and tool confidence, professionals can prioritize their remediation efforts accordingly. The AI-powered system also generates comprehensive HTML reports containing recommendations and reproduction steps for each vulnerability, making it easier for IT teams to address the issues.

A single risk interface allows users to filter vulnerabilities based on EPSS, CVSS, confidence, Risk, and solvability scores, providing a unified view of the security posture across all

scanners. This simplifies the process of managing vulnerabilities and enables organizations to focus on the most critical issues.

Furthermore, the proposed solution enables attack surface management by taking IP ranges or partial domains as input, and discovering all active IPs and websites within the specified range. This feature helps organizations to better understand their attack surface and identify potential vulnerabilities.

The study offers a comparative analysis of these methodologies with multiple different commercial vulnerability scanners, on different real environments from Dutch universities and SURF. Combined with interviews with their employees about how our tool compares with the state of the art regarding its risk scoring, reporting, and usability, the research provides valuable insights for professionals seeking to optimize their IT security protocols and strategies.

In conclusion, this research highlights the benefits of harnessing AI and open-source tools for enhanced IT security vulnerability assessment. By combining traditional vulnerability scanners with AI-powered prioritization and reporting, organizations can optimize their security protocols and strategies, leading to more robust and effective IT security management. The modular and scalable nature of the proposed solution ensures that it caters to organizations with varying security needs, making it an invaluable asset for IT professionals seeking to stay ahead of the curve in the ever-changing world of cybersecurity.