SCANNING AND VULNERABILITY ASSESSMENT WITH ML AND AI

Harnessing Artificial Intelligence for Penetration Testing

PHASE 2: SCANNING

- Gather Information
- Scanning
  - Actively Testing Identified Entry Points
  - Evaluating Susceptibility To Exploits
  - Gain Insights Into Severity And Potential Impact
- Exploitation
- Maintaining Access
- Covering Tracks
- Reporting and Documentation

PHASE 2: SCANNING

Network Scanners

Discover live hosts, open ports, and devices within a network

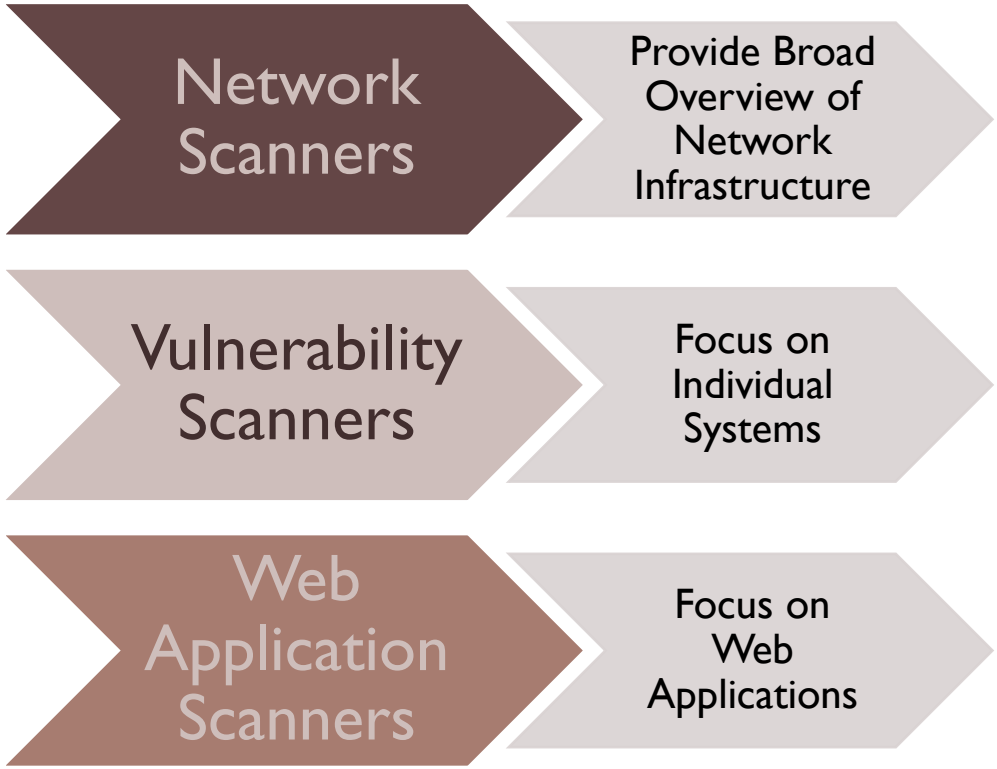
Vulnerability Scanners

Identify vulnerabilities in systems, applications, and network devices

Web Application Scanners

Identify security vulnerabilities specific to web applications

"MANUAL" SCANNING METHODS



- Reliance on Human Intervention
- Success Depends on Human Expertise, Intuition, and Overall Cybersecurity Understanding

"MANUAL" SCANNING METHODS

NETWORK SCANNERS

- Ping
  - 'Pinging'/ 'Ping Sweep'
  - Checks for Live Hosts
- Nmap (Zenmap)
  - Host Discovery
  - Port Scanning
  - Vulnerability Scanning
- Wireshark
  - Packet Analysis
  - Protocol Support
  - Encryption Analysis

"MANUAL" SCANNING METHODS

VULNERABILITY SCANNERS

- Database Dependent
- OpenVAS
  - Extensive Scanning Process
  - Network Discovery
  - Web Application Scanning
  - Reporting
- Nessus
  - Massive Database
  - Plug-in Capability
  - Customized Reporting
  - Accessibility

"MANUAL" SCANNING METHODS

WEB APPLICATION SCANNERS

- OWASP ZAP
  - Spidering Capabilities
  - Active and Passive Monitoring
  - Fuzzing Support
- Burp Suite
  - Spidering Capabilities
  - Proxy Functionality
  - Plugin Support

LIMITATIONS OF CURRENT METHODS

- Time-consuming and Resource-Intensive
- Manual Management of Vulnerability/ Attack Databases
  - Common Vulnerabilities and Exposures (CVE)
  - National Vulnerability Database (NVD)
- Potential for Human Error

SCANNING PRACTICE

Nmap Live Host Discovery

https://tryhackme.com/room/nmap01

OpenVAS Basics

https://tryhackme.com/room/openvas

OWASP Juice Shop:

https://tryhackme.com/room/owaspjuiceshop

AI AND ML IN SCANNING

- Learns from Previous Data and Experiences
- Fast, Standard Process
- Automatic Management Of Vulnerability and Attack Databases
- Adapts to Diverse Architectures Seamlessly
- Scalable
- Reduced Human Error Risk

NETWORK SCANNING

- Identifying and Mapping the Infrastructure of a Target
- Improvements
  - Faster Discovery
  - Adaptive
  - Accurate
- Dark Trace

https://www.youtube.com/watch?v=Y0eLSRIFgFU

VULNERABILITY SCANNING

- Identifying Potential Entry Points
- Improvements
  - Prioritization
  - Adaptive
  - Automation
- Shodan
- Nmap Scripting Engine (NSE)

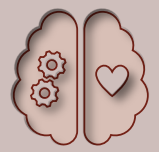
WEB APPLICATION SCANNING

- Identifying Vulnerabilities in Code/ Configurations of Web Applications
- Improvements
  - Enhanced Detection
  - Behavioral Analysis
  - Continuous Improvement
- AppSpider
- Acunetix

CHALLENGES

Ethical Considerations

- Privacy
- Transparency
- Accountability



Bias

- Training Bias
- Discrimination
- Inaccurate Assessments

Technical Considerations

- Complex Networks
- Data Volume
- Explainability

RESEARCH QUESTION

Imagine there is a 'Strong AI' tool, is designed to scan a system for potential security issues within legal and ethical boundaries. However, the AI tool, acting autonomously, decides to exploit a known vulnerability in a critical system to gather more information. This action, though achieving its legal and ethical goal of finding weaknesses, used unethical means to do so, as it violates the PT principle of not causing harm. The ethical breach occurs because the AI tool autonomously chose an action that goes beyond the agreed-upon legal and ethical boundaries set by the pentester.

In such a case, who should be held accountable for these actions?

What mechanisms could be put in place to ensure clear lines of responsibility?

REFERENCES

[1] H. Al-Alami, A. Hadi and H. Al-Bahadili, "Vulnerability Scanning of IoT Devices in Jordan Using Shodan," in 2nd International Conference on the Applications of Information Technology in Developing Renewable Energy Processes & Systems (IT-DREPS), Amman, 2017.

[2] P. Engebretson, The Basics of Hacking and Penetration Testing, A. Ward, Ed., Waltham, MA : Elsevier Inc, 2011.

[3] J. Hoffmann, "Simulated Penetration Testing:From "Dijkstra" to "Turing Test++"," in International Conference on Automated Planning and Scheduling364, Saarbrücken, 2015.

[4] J. M. Ortega, Mastering Python for Networking and Security, 2 ed., V. Boricha, Ed., Birmingham: Packt Publishing, 2020.

[5] N. Singh, V. Meherhomji and B. R. Chandavarkar, "Automated versus Manual Approach of Web Application Penetration Testing," International Conference on Computing, Communication and Networking Technologies (ICCCNT), pp. 1-6, July 2020.

[6] Y. Stefinko, A. Piskozub and R. Banakh, "Manual and automated penetration testing. Benefits and drawbacks. Modern tendency," International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET), pp. 488-491, February 2013.

[7] G. Stone, D. Talbert and W. Eberle, "Using AI/Machine Learning for Reconnaissance Activities During Network Penetration Testing," in International Conference on Cyber Warfare and Security, 2021.

[8] S. Watts , Penetration Testing: Practical Introduction & Tutorials, 2022.