S&Y Security labs

Uncovering 250+ Vulnerabilities with Active & Passive Scans

Our comprehensive approach combined active and passive scanning techniques, leveraging cutting-edge tools to uncover over 250 vulnerabilities across our clients' systems since February 2024.

S **by Salah Khamassi**

Active vs passive scan analysis

Active analysis interacts directly with the target systems to detect vulnerabilities. This is a more detectable but more thorough method.

Passive analysis monitors network traffic and system behavior without interaction. This is a stealthier method but may miss some issues.

Combining the two methods has enabled a comprehensive security assessment.

Tools Powering Our Approach

OWASP ZAP

Web application security scanner for identifying vulnerabilities.

Nmap

Network mapping and security auditing tool.

Intruder

Cloud-based vulnerability scanner for continuous monitoring.

Wireshark

Network protocol analyzer for passive traffic analysis.

Key Findings and Insights

1

256 Vulnerabilities Identified

Ranging from low to critical severity.

2

Deeper Security Posture Understanding

Gained comprehensive visibility into potential risks.

3

Immediate Fixes and Long-Term Strategy

Addressed critical issues and developed a continuous improvement plan.

Safeguarding Digital Assets

Our comprehensive security assessment strategy, combining active and passive scanning techniques, has uncovered over 250 vulnerabilities across our clients' systems. This highlights the critical importance of proactively identifying and addressing potential security risks to effectively safeguard digital assets.

By leveraging a suite of advanced tools, including OWASP ZAP, Nmap, Intruder, Wireshark and Shodan among others, we have gained a deeper understanding of our clients' security posture regarding their internet facing assets. This multi-layered approach, encompassing both interactive and passive analysis, has enabled us to detect a wide range of vulnerabilities, from low to critical severity.

The insights gained from this thorough assessment have not only allowed us to address the immediate threats, but also to develop a long-term strategy for continuous improvement and strengthening our clients' overall security resilience. Our mission is to ensure that our clients' digital assets remain safe and secure, protecting them from evolving cyber threats.

S&Y Security Labs**TM** | May 2024