

# Passive Vulnerability Assessment

## What is Passive Vulnerability Assessment?

Passive vulnerability assessment is a non-intrusive method of identifying potential security weaknesses in an organization's digital assets without actively engaging with the systems or networks. This approach gathers information from publicly available sources and network traffic observations without sending any data or probes to the target systems.

## How We Conduct Passive Vulnerability Assessment

As part of our comprehensive attack surface management, we perform passive vulnerability assessments to identify potential risks without impacting your systems. Here's our approach:

- 1. Information Gathering:**
  - We collect publicly available information about your digital assets.
  - This includes domain names, IP addresses, subdomains, and associated services.
- 2. External Footprint Analysis:**
  - We analyze your organization's external-facing infrastructure.
  - This includes web servers, email servers, DNS configurations, and other public-facing services.
- 3. Network Traffic Observation:**
  - We monitor network traffic patterns without interfering with the data flow.
  - This helps identify potential vulnerabilities in network protocols and configurations.
- 4. OSINT (Open Source Intelligence) Techniques:**
  - We utilize various open-source intelligence gathering methods.
  - This includes searching public databases, forums, and social media for potential security-related information.

## 5. **SSL/TLS Analysis:**

- We examine SSL/TLS configurations of your web services.
- This helps identify weak encryption protocols, expired certificates, or misconfigurations.

## 6. **Header Analysis:**

- We analyze HTTP headers of your web applications.
- This can reveal information about the technologies in use and potential misconfigurations.

## 7. **Passive Port Scanning:**

- We identify open ports and services without actively probing your systems.
- This is done through analysis of publicly available scan data and passive network observations.

## 8. **Third-Party Service Assessment:**

- We evaluate the security posture of third-party services connected to your infrastructure.
- This includes cloud services, CDNs, and other external dependencies.

## 9. **Historical Data Analysis:**

- We review historical data from various sources to identify past vulnerabilities or incidents.
- This can reveal patterns or recurring issues in your security posture.

## 10. **Vulnerability Correlation:**

- We correlate the gathered information with known vulnerability databases.
- This helps identify potential vulnerabilities based on the technologies and configurations in use.

## 11. **Reporting and Risk Assessment:**

- We compile a comprehensive report of our findings, including:
  - Potential vulnerabilities identified
  - Risk assessment for each vulnerability
  - Recommendations for further investigation or remediation
- The report prioritizes issues based on their potential impact and likelihood of exploitation.

By conducting passive vulnerability assessments, we provide valuable insights into your security posture without any risk of disrupting your operations. This approach allows for continuous monitoring and early detection of potential security issues in your attack surface.

---

Revision #1

Created 19 September 2024 08:55:44 by Admin

Updated 19 September 2024 08:59:18 by Admin