

# Passive Vulnerability

- [Passive Vulnerability Assessment](#)
- [Risks Identified in Passive Vulnerability Assessment](#)
- [Passive VA Risk Mitigation](#)

# 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.

# Risks Identified in Passive Vulnerability Assessment

Passive vulnerability assessment is a crucial component of attack surface management. It allows for the identification of potential security weaknesses without actively engaging with the target systems. This knowledge base article focuses on three primary areas of risk commonly identified through passive vulnerability assessment.

## 1. Identifying CVEs and Outdated Software/Services

Passive vulnerability assessment can reveal the use of software or services with known vulnerabilities, often identified by Common Vulnerabilities and Exposures (CVE) numbers.

### How we identify:

- Analyze version information disclosed in HTTP headers, HTML source code, or other publicly accessible information.
- Cross-reference detected software versions with known vulnerability databases.
- Examine server responses for signatures of specific software versions.

### Risks:

- Exposure to known exploits targeting specific vulnerabilities.
- Increased likelihood of successful attacks due to publicly available exploit code.
- Potential for easy compromise of systems and data.

### Impact:

- Unauthorized access to systems or data.
- Potential for malware infection or data exfiltration.

- Compliance violations due to failure to maintain up-to-date software.

## 2. Risks from Open Ports and Exposed Services

Open ports and exposed services can significantly expand an organization's attack surface, providing potential entry points for attackers.

### How we identify:

- Analyze publicly available scan data from services like Shodan or Censys.
- Examine DNS records for unexpected service entries.
- Passively monitor for services responding on non-standard ports.

### Risks:

- Exposure of internal services not intended for public access.
- Potential for unauthorized access to sensitive systems or data.
- Increased attack surface for potential exploits.

### Impact:

- Unauthorized data access or system compromise.
- Potential for lateral movement within the network if an exposed service is compromised.
- Violation of security principles like least privilege and defense-in-depth.

## 3. Shadow IT and Rogue Asset Risks

Shadow IT refers to the use of systems, devices, or services without explicit organizational approval, while rogue assets are unknown or unmanaged devices connected to an organization's network.

# How we identify:

- Discover unknown subdomains through DNS analysis.
- Search for company-related assets on public cloud services.
- Detect digital certificates associated with the organization but not in the official asset inventory.

# Risks:

- Unmanaged and potentially vulnerable assets increasing the attack surface.
- Data storage or processing on unapproved systems, leading to potential data leaks.
- Bypass of established security controls and monitoring systems.

# Impact:

- Increased difficulty in maintaining a comprehensive security posture.
- Potential compliance violations due to uncontrolled data handling.
- Creation of unexpected entry points for attackers.

By focusing on these three key areas, organizations can significantly improve their security posture through passive vulnerability assessment. This non-intrusive approach provides valuable insights into potential risks without actively engaging with systems, allowing for proactive security measures and more effective attack surface management.

# Passive VA Risk Mitigation

## Risk Mitigation Strategies

Addressing the vulnerabilities identified through passive vulnerability assessment is crucial for improving an organization's security posture. Here are specific mitigation strategies for each of the key risk areas:

### 1. Mitigating CVEs and Outdated Software/Services Risks

- Implement a robust patch management process to ensure timely updates of all software and services.
- Establish a regular vulnerability scanning routine to identify new CVEs quickly.
- Create and maintain an up-to-date inventory of all software and their versions used in the organization.
- Implement a software end-of-life policy to plan for replacement of outdated or unsupported software.
- Use virtual patching or web application firewalls (WAF) as temporary measures while planning updates.
- Conduct regular security assessments to identify and prioritize vulnerabilities for remediation.

### 2. Mitigating Risks from Open Ports and Exposed Services

- Implement the principle of least privilege by closing all unnecessary ports and services.
- Use firewalls and access control lists (ACLs) to restrict access to necessary ports and services.
- Regularly audit open ports and exposed services to ensure they are still required and secure.
- Implement network segmentation to isolate critical services from public-facing networks.
- Use strong authentication mechanisms, such as multi-factor authentication, for accessing exposed services.

- Employ intrusion detection and prevention systems (IDS/IPS) to monitor and protect exposed services.
- Implement proper logging and monitoring for all exposed services to detect potential security incidents quickly.

## 3. Mitigating Shadow IT and Rogue Asset Risks

- Develop and enforce clear policies on the use of unauthorized software, services, and devices.
- Implement network access control (NAC) solutions to detect and manage unknown devices connecting to the network.
- Conduct regular network scans and asset discovery to identify unknown or unauthorized assets.
- Use cloud access security brokers (CASBs) to discover and control the use of shadow IT in cloud services.
- Implement data loss prevention (DLP) solutions to monitor and control data flow to unauthorized services.
- Provide approved alternatives to common shadow IT solutions to meet employee needs securely.
- Conduct regular security awareness training to educate employees about the risks of shadow IT and the importance of following security policies.
- Establish a process for employees to request and rapidly receive approval for new software or services they need.

By implementing these mitigation strategies, organizations can significantly reduce the risks identified through passive vulnerability assessment. It's important to note that security is an ongoing process, and these strategies should be regularly reviewed and updated to address new and evolving threats.