

Understanding Assets Scan Results

The scan results provide a comprehensive list of assets that are directly associated with the initial scanned domain. These assets include subdomains, IP addresses, open ports, and the technologies used on these services. Monitoring these assets is essential for maintaining the security and integrity of your organization's digital infrastructure. Here's a breakdown of the information provided in each column:

1. **# (Index):**

This is a sequential number assigned to each asset in the list. It serves as a reference point for quickly locating and discussing specific assets within the scan results.

2. **IP ADDRESS:**

The IP address indicates the numerical label assigned to each asset on the network. It identifies the specific server or host where the subdomains are hosted. Monitoring IP addresses is crucial for detecting unauthorized changes or identifying potential vulnerabilities in your network infrastructure.

3. **DOMAIN(S):**

This column lists the subdomains associated with the main scanned domain. These subdomains often serve various functions such as hosting web services, email services, or internal tools. It's important to monitor subdomains to ensure they are properly secured, as they can be prime targets for attackers if left unprotected.

4. **PORTS:**

Ports are communication endpoints on a server that allow different services to interact over the network. This column lists the open ports detected for each asset, such as `80/www-http` and `443/https`. Open ports can reveal what services are running on the server. For example, port 80 is typically used for HTTP traffic, while port 443 is used for HTTPS traffic. Identifying open ports helps in assessing potential security risks, such as unprotected services or outdated software.

5. **TECHNOLOGIES:**

This column identifies the technologies and software used on the server for each asset. It may include web servers like Microsoft IIS, Nginx, or Google HTTPD, as well as services provided by content delivery networks like AkamaiGHost. Knowing which technologies are in use helps assess the security posture of each asset. It can also identify outdated or vulnerable software that may need to be updated to protect against security threats.

Example Analysis:

- **Asset 1:**

- **IP Address:** 23.197.153.80
- **Domains:** image.info.demodata.com, image.demodata.com
- **Ports:** 80/www-http, 443/https
- **Technologies:** AkamaiGHost
- **Analysis:** This asset is hosted on the IP address 23.197.153.80, with subdomains that appear to serve images or media content. It uses AkamaiGHost, which suggests that Akamai's content delivery network (CDN) is being used to optimize and secure content delivery.

- **Asset 2:**

- **IP Address:** 87.239.13.42
- **Domains:** mta-sts.demodata.com
- **Ports:** 25/smtp, 80/www-http, 443/https
- **Technologies:** nginx
- **Analysis:** This asset hosts the subdomain mta-sts.demodata.com and runs on multiple ports including 25 (SMTP), indicating it handles email services. The use of Nginx suggests a robust and flexible web server configuration. Ensuring proper security configurations on the SMTP port is crucial to prevent email-based attacks.

By analyzing these assets, you can gain insights into your domain's infrastructure and identify areas that may require additional security measures. This process helps in maintaining a secure environment by monitoring changes, assessing vulnerabilities, and ensuring that each asset adheres to the organization's security policies.

Revision #3

Created 16 September 2024 11:59:08 by Raphael

Updated 16 September 2024 12:13:52 by Raphael