Response Metadata, Data Component DC0106

Archived: 2026-04-05 16:34:48 UTC

Contextual information about an Internet-facing resource collected during a scan, including details such as open ports, running services, protocols, and versions. This metadata is typically derived from interpreting scan results and helps build a profile of the targeted system. Examples:

- Port and Service Details:
  - Open ports (e.g., 22, 80, 443).
  - Identified services running on those ports (e.g., SSH, HTTP, HTTPS).
- Service Versions: Detected software version information (e.g., Apache 2.4.41, OpenSSH 8.2).
- Operating System Information: OS fingerprinting data (e.g., Linux Kernel 5.4.0).
- TLS/SSL Certificate Data: Information about the TLS/SSL certificate, such as the expiration date, issuer, and cipher suites.

Data Collection Measures:

- Scanning Tools:
  - Nmap: Collects port, service, and version information using commands like nmap -sV .
  - Masscan: High-speed scanning tool for discovering open ports and active services.
  - Zmap: Focused on large-scale Internet scanning, collecting metadata about discovered services.
  - Shodan API: Retrieves scan metadata for publicly exposed devices and services.
- Network Logs:
  - Use logs from firewalls, intrusion detection systems (IDS), or intrusion prevention systems (IPS) to gather metadata from scan attempts. Example: Zeek or Suricata logs for incoming scan traffic.
- OSINT Platforms: Platforms like Censys, GreyNoise, or Shodan provide aggregated metadata about Internet-facing resources.
- Cloud Metadata Services: AWS Security Hub, Azure Monitor, or GCP Security Command Center can collect and centralize scan-related metadata for Internet-facing resources in cloud environments.
