SSL Scanning

Overview of SSL Certificate Scanning

As part of our comprehensive asset discovery and vulnerability assessment process, we scan your organization's digital assets to identify and analyze SSL/TLS certificates. This process helps ensure the security and compliance of your web services.

How We Scan for SSL Certificates

1. **Asset Discovery**:
   - We start by identifying all domains and subdomains associated with your organization.
   - This includes public-facing web servers, mail servers, and other services that use SSL/TLS.
2. **Port Scanning**:
   - We scan common SSL/TLS ports (e.g., 443 for HTTPS, 25 for SMTP) across all identified IP addresses.
3. **SSL/TLS Handshake**:
   - For each responsive port, we initiate an SSL/TLS handshake to retrieve the certificate information.
4. **Certificate Chain Analysis**:
   - We analyze the entire certificate chain, including root and intermediate certificates.
5. **Certificate Data Extraction**:
   - We extract key information from each certificate, including:
     - Subject (domain name)
     - Issuer (Certificate Authority)
     - Valid from/to dates
     - Key size and algorithm
     - Serial number

What We Look For

1. **Certificate Expiry**:
    - We identify certificates that are expired or nearing expiration (e.g., within 30 days).
2. **Weak Cryptography**:
    - We flag certificates using outdated algorithms (e.g., SHA-1) or insufficient key sizes.
3. **Hostname Mismatch**:
    - We check if the certificate's subject matches the hostname it's served from.
4. **Self-Signed Certificates**:
    - We identify self-signed certificates, which are generally not trusted for public-facing services.
5. **Revoked Certificates**:
    - We check certificate revocation status using CRL and OCSP.
6. **Vulnerable SSL/TLS Versions**:
    - We detect if servers support outdated and vulnerable SSL/TLS versions (e.g., SSL 3.0, TLS 1.0).
7. **Certificate Transparency**:
    - We verify if certificates are logged in Certificate Transparency logs, as required by many browsers.
8. **Wild Card Certificates**:
    - We identify and flag the use of wildcard certificates, which can pose additional risks if compromised.

Reporting

Our scanning process generates a comprehensive report that includes:

- A list of all discovered SSL/TLS certificates across your assets
- Details of each certificate, including expiry dates and potential issues
- Prioritized list of certificates requiring attention (e.g., near expiry, vulnerable configurations)
- Recommendations for addressing identified issues

Revision #1
Created 19 September 2024 10:14:40 by Admin
Updated 19 September 2024 10:30:27 by Admin