Understanding Scanning results

Understanding Vulnerability Scanning results

It's essential not only to identify vulnerabilities in your attack surface but also to provide you with the most effective information to resolve these issues. Depending on the severity of the vulnerability, you might want to address it directly once a vulnerability is detected by ReConfirm.

All identified vulnerabilities can be found under the "Vulnerabilities" section in the ReConfirm tool. Each finding is assigned a severity level based on its CVSS score or potential technical impact if no CVSS score is available.

To view the results, simply click on the "view" button of the latest scan within the vulnerabilities page. Here, you'll find three cards:

Details:
This section provides a comprehensive overview of the vulnerability, including information such as the vulnerability type, location, and potential impact. It gives you a clear understanding of what the issue is and where it was found, helping you assess its relevance to your system. The details include specific data points to help you prioritise the vulnerability effectively.

Results:
Under this card, you'll find the technical findings from the scan. It includes the raw data and insights gathered during the scan process, such as payloads used, affected endpoints, or any additional evidence collected. This detailed output allows you to dive deep into the scan results, helping you understand the full scope of the vulnerability and how it was discovered.

Mitigation:
The Mitigation card offers actionable guidance on how to address and resolve the identified vulnerability. It outlines recommended steps and best practices to remediate the issue, tailored to the specific context of the finding. By providing clear instructions, this section helps you quickly implement fixes to secure your environment.

You can export selected findings in CSV, TXT, or XML format to share with colleagues, partners, or clients, or send them directly through email with a personalised message.

Understanding Email Security Results

The Email Security section presents the results of security checks on key email authentication protocols, including DMARC, SPF, MX, and DKIM. This information helps users assess the email security configuration of the scanned domain, ensuring that measures are in place to prevent email spoofing and protect against phishing attacks.

DMARC (Domain-based Message Authentication, Reporting, and Conformance):
DMARC is an email authentication protocol that builds on SPF and DKIM to ensure that emails sent from your domain are properly authenticated. It provides domain owners with a mechanism to specify how to handle emails that fail authentication checks, offering options such as rejecting or quarantining suspicious messages. DMARC also generates reports on email authentication activity, giving you insights into who is sending emails on behalf of your domain and helping identify potential abuse.

SPF (Sender Policy Framework):
SPF is an email authentication method that allows domain owners to define which IP addresses or servers are authorized to send emails on their behalf. This is done by publishing an SPF record in the domain's DNS settings, listing the permitted mail servers. When an email is received, the recipient's mail server checks the SPF record to verify that the email came from an authorized source. If the sending server is not listed in the SPF record, the email may be marked as spam or rejected.

MX (Mail Exchanger) Records:
MX records are a type of DNS record that specify the mail servers responsible for receiving emails on behalf of a domain. They direct incoming email to the correct mail servers, ensuring that messages are delivered to the right destination. Proper configuration of MX records is crucial for ensuring reliable email delivery, as incorrect settings can lead to misrouted or undelivered emails.

DKIM (DomainKeys Identified Mail):
DKIM is an email authentication technique that allows the sender to sign their emails with a digital signature. This signature is included in the email header and is used to verify that the message was not altered in transit. The public key required to verify the signature is published in the sender's DNS records. By using DKIM, recipients can be confident that the email genuinely originated from the stated domain and was not tampered with during transmission.

ReConfirm checks a default list of DKIM selectors to verify the authenticity of your emails. If your organization uses custom selectors for DKIM, you can add them for scanning by clicking "Check Selectors" and entering the relevant selectors. This ensures a comprehensive evaluation of your

email security configuration.

Understanding Similar Domains Results

Similar Domains:
The listed domains closely resemble the scanned domain in text or pronunciation. It is crucial to monitor these "lookalike domains," as they pose significant risks to your organization. Lookalike domains are often used by malicious actors to exploit unsuspecting users, leading to various security and reputational threats.

The scan results provide an overview of domains similar to the scanned domain, highlighting key technical details such as their geographical location, DNS records, status codes, and more. Here's a breakdown of each element in the results:

1. **DOMAIN:**
   This column lists the similar domains identified in the scan. These domains have names that are either visually or phonetically similar to the scanned domain, which can pose a risk if they are used for malicious activities.
2. **GEO IP:**
   This indicates the geographical location of the server hosting the domain, identified by its IP address. Knowing the server's location can provide insights into where the domain is operated from, which may help assess the potential risk or legitimacy of the domain.
3. **DNS A RECORD(S):**
   The A record is a type of DNS record that maps a domain name to its corresponding IP address. This column shows the IP addresses associated with each domain, helping identify where the domain is hosted. Multiple IP addresses may indicate different hosting setups, such as load balancing or geographical distribution.
4. **DNS MX RECORD(S):**
   MX (Mail Exchanger) records are DNS records that specify the mail servers responsible for receiving email on behalf of the domain. This column lists the MX records, showing where the domain directs its email traffic. The presence or absence of MX records can indicate whether the domain is configured to send or receive emails, which is relevant for assessing the risk of phishing attacks.
5. **DNS NS RECORD(S):**
   NS (Name Server) records specify the authoritative name servers for the domain. These servers handle queries for the domain's DNS records. This column lists the NS records, providing information about the domain's DNS infrastructure. The name servers can reveal whether a domain uses a reputable DNS provider or a potentially suspicious one.
6. **PAGE TITLE:**
   The page title is the text that appears on the browser tab when visiting the domain's

website. It provides a brief description of the website's content or purpose. This column displays the title found on the homepage of each domain. A title that closely resembles the scanned domain's legitimate site may indicate an attempt to impersonate it.

7. **STATUS CODE:**
   The status code indicates the HTTP response code returned by the domain when accessed. A status code of **200** means the server successfully returned the requested webpage. Other status codes, such as 404 (Not Found) or 301 (Redirect), can provide clues about the domain's functionality and purpose.
8. **SCREENSHOT:**
   This column provides a screenshot of the homepage of each domain. Visual inspection of the screenshot can help identify if the domain is a clone or imitation of the legitimate site, or if it contains suspicious or malicious content.

Example Analysis:

- **demodata.com**
  - Located in the United States with an IP address of 192.168.1.100.
  - It has DNS A and NS records but no MX records, indicating it may not be configured to handle email.
  - The page title "Welcome to DemoData" and a status code of 200 suggest an operational website. Further inspection of the site’s content is recommended to ensure it's not attempting to impersonate a legitimate brand.
- **demodat.com**
  - Hosted in Canada at IP address 172.16.254.1.
  - Lacks MX records, which may indicate it is not set up for email communication.
  - The status code 200 and page title "DemoDat - Your Data Solution" indicate the site is live. Visual inspection of the website and its content would be necessary to determine if it poses any threat or attempts to mimic a legitimate site.

By reviewing these details, you can assess the potential risks each similar domain poses, such as phishing, impersonation, or hosting malicious content. This analysis aids in prioritizing domains for closer monitoring or potential action.

Understanding Associated Domains Results

The "Associated Domains" section provides a list of domains that are either connected to the scanned domain or have been seen interacting with it in various capacities. Monitoring these associated domains is crucial as they can give insights into your organization's broader online presence and interactions. Here’s what this section covers in more detail:

Associated Domains:
These domains are linked to your main business operations but might serve different functions. They could include domains used for marketing campaigns, customer support portals, special projects, or subsidiary websites. Understanding the role of these associated domains helps in identifying the full scope of your organization's digital footprint, ensuring consistent security practices across all related properties.

Third-Party Vendors:
These are domains owned and operated by external entities that your main website or business interacts with. They include services such as analytics providers, customer relationship management (CRM) systems, advertising networks, or content delivery networks (CDNs). While these domains provide essential services, they can also introduce potential security risks, especially if they are not properly managed or monitored.

Scan Results Explanation:

1. **DOMAIN:**
   This column lists the associated domains identified in the scan. These domains are either directly related to your organization or frequently interact with your main domain. Regularly reviewing these domains helps ensure they align with your security and operational policies.
2. **TIMES SEEN:**
   This indicates how many times the associated domain has been observed interacting with your scanned domain. A higher number suggests more frequent interaction, which can highlight the domain's importance or indicate a strong association with your operations. Regular monitoring of these interactions is vital to identify any unusual or unexpected activity.
3. **PAGE TITLE:**
   The page title provides a brief description of the content or purpose of the associated domain’s website. It can give a quick insight into the domain's function. For example, a

title like "Employee and Customer Identity Solutions" suggests a domain related to identity management, indicating its role in the context of your operations.

4. **STATUS CODE:**
   The status code represents the HTTP response code returned when accessing the domain. A status code of **200** indicates that the server successfully returned the requested webpage, suggesting that the domain is currently live and operational. Other status codes can help identify domains that may no longer be active or are redirecting to different resources.
5. **SCREENSHOT:**
   This provides a visual snapshot of the associated domain’s homepage. Reviewing these screenshots can help quickly identify if the domain appears legitimate, if it accurately reflects the expected content, or if it shows signs of malicious activity, such as hosting misleading or harmful content.

Example Analysis:

- **windows.net**
  - Seen 36 times, suggesting frequent interaction with your main domain.
  - The page title ".NET | Build. Test. Deploy." indicates it's related to development or hosting services.
  - A status code of 200 confirms the site is live, and further review can verify its role within your organization's ecosystem.
- **outlook.com**
  - Seen 27 times, which is common for a widely used email and communication service.
  - No available page title or status code, indicating that it may serve a specific purpose such as email redirection or an API endpoint rather than hosting public-facing content.

By analyzing these associated domains, you gain a better understanding of your organization's online ecosystem. This can help identify potential security risks, ensure proper usage of third-party services, and maintain a secure and consistent online presence.

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.

Understanding Credential Leaks Results

The "Credential Leaks" section provides information on email addresses associated with the scanned domain that have appeared in known data breaches. Monitoring credential leaks is crucial for understanding potential security risks and taking action to protect user accounts and sensitive information. Here’s a breakdown of each column in the scan results:

1. **EMAILS:**
   This column lists the email addresses that have been found in data breaches. These emails are associated with the scanned domain, and their appearance in breaches indicates potential exposure of sensitive information. Monitoring these email addresses helps identify accounts that may be at risk and need immediate attention, such as password changes or enhanced security measures.
2. **KNOWN BREACHES:**
   This column identifies the specific data breaches where the email addresses were found. The breaches may range from well-known websites, such as social media platforms and online services, to lesser-known sources. Understanding the origin of the breach can help assess the severity of the exposure and the types of data that may have been compromised.
3. **SOURCE(S):**
   The sources indicate where the information about the breach was obtained. This could include data breach repositories, security forums, or direct notifications from the affected services. Knowing the sources helps in verifying the authenticity of the breach information and taking appropriate steps to mitigate risks.
4. **LEAKED PASSWORD:**
   This column indicates whether a password associated with the breached email was leaked. The use of "**********" signifies that the password has been detected but is not displayed for security reasons. If passwords are known to be leaked, it’s imperative to change them immediately and implement stronger security practices like multi-factor authentication (MFA).
5. **LAST BREACH:**
   The date of the most recent breach involving the email address is listed here. This information helps in determining how current the threat is and whether immediate action is needed. For example, recent breaches may require prompt responses, such as notifying affected users and enforcing password resets.

Stealer Logs:

Stealer Logs refer to data collected by malicious software, known as information stealers, which infiltrate a victim's device to harvest sensitive information. These logs typically contain a wide range of data, including usernames, passwords, browsing history, cookies, and even autofill information from web browsers. Stealer logs can be especially dangerous because they often capture data directly from the user's device before it is encrypted or stored securely. This makes them a potent source of sensitive information for cybercriminals.

When an email appears in stealer logs, it indicates that the credentials or sensitive data were not just exposed in a typical data breach but were actively stolen from a compromised device. This poses a significant threat, as it may include real-time or recent data, increasing the risk of immediate exploitation. Organizations should take the presence of stealer logs very seriously by:

- Immediately resetting the passwords associated with the affected accounts.
- Running comprehensive security scans on the compromised device(s).
- Implementing multi-factor authentication (MFA) to protect against further unauthorized access.

Example Analysis:

- **Email:** peet.greenroad@demodata.com
  - **Known Breaches:** Unknown
  - **Source(s):** Unknown/Stealer Logs/Known
  - **Leaked Password:** Yes
  - **Last Breach:** Unknown
  - **Analysis:** This email address has appeared in a data breach, but the specific source and date of the breach are not identified. Immediate action should include changing the password and reviewing the account for any unauthorized activity.

By regularly reviewing the "Credential Leaks" data, including stealer logs, you can take proactive measures to secure affected accounts, mitigate the risk of unauthorized access, and implement stronger security practices such as regular password updates, device security audits, and multi-factor authentication (MFA).

Understanding Subdomains Results

Subdomain Scan Results

The Subdomain Scan provides a comprehensive overview of the subdomains associated with the scanned domain. Monitoring subdomains is crucial as they often host various services and applications that can be potential targets for attackers if not properly secured. The scan results start with an overview of all discovered subdomains, highlighting key information such as IP addresses, open ports, HTTP status codes, content length, and more. Clicking on a specific subdomain takes you to its detailed analysis page.

Overview of Subdomains:

This section lists all subdomains discovered during the scan. Each entry provides essential information to quickly assess the subdomain's characteristics:

1. **SUBDOMAIN:**
   The name of the subdomain found under the main domain, such as `planner.demodata.com`. Subdomains typically serve different functions within an organization, such as hosting web applications, APIs, or administrative portals.
2. **IP ADDRESS:**
   The IP address associated with the subdomain, indicating where it is hosted. While the IP is not shown here for security reasons, it helps identify the server's location and assess potential security measures in place.
3. **OPEN PORTS:**
   The list of open ports on the subdomain, such as `80/www-http` and `443/https`. Open ports indicate which services are accessible and may need further scrutiny to ensure they are securely configured.
4. **HTTP STATUS:**
   The HTTP response code returned when the subdomain is accessed. A status code of `200` indicates a successful response, meaning the subdomain is live and serving content.
5. **CONTENT LENGTH:**
   The size of the response content, providing insight into the volume of data the subdomain returns. Large content length may indicate a complex page or application.
6. **PAGE TITLE:**
   The title of the web page served by the subdomain, giving a brief idea of its purpose. For example, "Simple Planner v10.65.4" suggests a planning application.

7. **SCREENSHOT:**
   A visual capture of the subdomain's homepage, useful for quickly identifying the nature of the content and potential risks, such as impersonation or phishing.

Subdomain Detail Page:

Clicking on a specific subdomain, such as `planner.demodata.com`, takes you to a detailed analysis page that provides an in-depth view of the subdomain's configuration and security posture.

Overview of `planner.demodata.com`

1. **Subdomain Information:**
   - **Full URL:** The complete URL for accessing the subdomain, e.g., `https://planner.demodata.com`.
   - **Page Title:** A brief description of the web page, indicating the subdomain's function.
   - **Content Length:** Size of the content returned by the subdomain.
   - **HTTP Response Code:** Indicates the HTTP status, such as `200` for a successful request.
2. **IP Addresses:**
   Lists the associated IP address(es) hosting this subdomain. The IP address information is crucial for tracking hosting providers and understanding the subdomain's network setup.
3. **Ports:**
   Displays open ports on the subdomain, revealing the services running, such as HTTP (`80`) or HTTPS (`443`). Open ports must be secured to prevent unauthorized access.
4. **Services:**
   Identifies the software and technologies in use on the subdomain, such as `nginx/1.25.3`. Knowing the services helps in assessing the security posture and checking for known vulnerabilities.
5. **Vulnerabilities Discovered:**
   The number of vulnerabilities found on the subdomain. Each vulnerability is listed with its severity level and the URL where it was discovered, aiding in prioritizing security efforts. An example of a critical vulnerability that may be discovered is:
   - **CVE-2021-44228 - Apache Log4j Vulnerability:**
     A critical vulnerability in Apache Log4j identified by CVE-2021-44228 has been publicly disclosed, potentially allowing for remote code execution in impacted Elasticsearch 5 installations. This severe flaw can be exploited by attackers to execute arbitrary code, leading to full system compromise. Immediate remediation is necessary, such as updating Log4j to the latest patched version.
6. **Missing Security Headers Grade:**
   A grade indicating the presence or absence of critical security headers. A low grade, such as "F," means essential security headers are missing, increasing the risk of attacks like cross-site scripting (XSS) or clickjacking.

7. **Suffixes Discovered:**
   Lists any URL suffixes found during the scan. These suffixes can point to accessible directories or files that may expose sensitive information.
8. **SSL Grade:**
   Assesses the quality of the SSL/TLS configuration for the subdomain. A "N/A" or low grade indicates potential issues with encryption, putting data transmission at risk.

Subdomain Vulnerabilities:

Provides a detailed overview of the vulnerabilities detected on the subdomain. Each vulnerability is listed with its severity and the URL where it was found. For instance, in addition to informational findings like technology detection, a critical vulnerability like the Apache Log4j exploit (CVE-2021-44228) indicates an urgent need for remediation to prevent remote code execution attacks.

Header Overview:

Displays a list of missing security headers that could improve the subdomain's security posture. Headers such as `Content-Security-Policy` or `X-Frame-Options` are crucial for protecting against attacks like XSS and clickjacking.

Suffixes Found:

Lists any suffixes (e.g., `example.com/admin`) discovered during the scan, which can expose additional entry points to the subdomain.

SSL/TLS Information:

Provides details about the SSL/TLS configuration of the subdomain, ensuring secure data transmission. No data indicates that an SSL scan is needed to evaluate the security of encrypted connections.

Response Information:

Shows the HTTP response headers returned by the subdomain, including information about the server, cookies, and security configurations. This helps in understanding how the server is configured and identifying potential security gaps.

Example Analysis:

- **Subdomain:** `planner.demodata.com`
  - **Open Ports:** 80, 443 (indicating HTTP and HTTPS services)
  - **Services:** Nginx/1.25.3
  - **Vulnerabilities:** 10 discovered, including critical vulnerabilities like the Apache Log4j (CVE-2021-44228) exploit that allows for remote code execution.

- **SSL Grade:** N/A
- **Analysis:** This subdomain runs a web application accessible over HTTP and HTTPS. It has multiple vulnerabilities, including a critical issue with Apache Log4j, which allows for remote code execution and must be addressed immediately. Other issues, such as missing security headers, further result in a low security grade. Urgent action is recommended, including patching Log4j, updating server software, and implementing necessary security headers to secure this subdomain.

By regularly monitoring subdomains and addressing detected vulnerabilities, including critical ones like the Apache Log4j exploit, you can strengthen your organization’s security posture, protect sensitive information, and prevent potential exploitation by attackers.

Understanding Inactive Subdomains Results

The Subdomains - Inactive Results section highlights subdomains that are either currently unresolved or offline. Monitoring these inactive subdomains is crucial for understanding potential risks and managing your organization's attack surface. Even though these subdomains may not be actively in use, they can still pose security risks if reactivated without proper security measures in place.

Unresolved Subdomains:

Unresolved subdomains are those that could not be resolved during the scan, meaning they do not currently point to an active IP address. However, based on historical data, these subdomains existed in the past. ReConfirm continues to monitor these subdomains to detect any changes that might make them active again.

1. **Total Unresolved Subdomains:**
   The total count of unresolved subdomains detected during the scan. For example, if ReConfirm identified a total of **589** unresolved subdomains, these are now flagged for monitoring.
2. **Subdomains List:**
   A detailed list of unresolved subdomains, such as `expiredjs.demodata.com` and `backupserver.demodata.com`. Although these subdomains are inactive, they may be unintentionally reactivated in the future. When an inactive subdomain becomes resolvable again, ReConfirm will detect the change and add it back to the active attack surface. Monitoring unresolved subdomains is essential to prevent unauthorized reactivation and potential exploitation by attackers.
   Example Subdomains:
   - `expiredjs.demodata.com`
   - `legacyservice.demodata.com`
   - `archive.demodata.com`
3. **Potential Risks:**
   These subdomains, if reactivated without proper security measures, can become an entry point for attackers. It is essential to periodically review and assess the need for these subdomains to avoid accidental exposure of outdated or vulnerable services.

Offline Subdomains:

Offline subdomains are those that could be resolved to an IP address but were not reachable during the scan. This could be due to several reasons, such as being behind a firewall, the server being offline, or network configuration issues.

1. **Total Offline Subdomains:**
   The total count of offline subdomains detected during the scan. For instance, if ReConfirm found **13** offline subdomains, these are now flagged for further review.
2. **Subdomains List:**
   A list of offline subdomains with their resolved IP addresses. These subdomains were detected but could not be probed, meaning ReConfirm could not scan them for vulnerabilities. This can occur if the subdomain is protected by a firewall or if the server is not responding.
   Example Offline Subdomains:
   - **Subdomain:** `mail.demodata.com`
     - **Resolved IP:** 192.168.1.1
   - **Subdomain:** `archive.demodata.com`
     - **Resolved IP:** 10.0.0.1
   - **Subdomain:** `api.demo2.demodata.com`
     - **Resolved IP:** 172.16.0.2
3. **Potential Risks and Recommendations:**
   - **Behind a Firewall:** If a subdomain is behind a firewall, evaluate whether it needs to be externally resolvable and reachable. If not, consider removing it from external DNS to minimize exposure.
   - **Offline or Non-Responsive:** If a subdomain is offline or not responding, assess whether it is still needed. If it is obsolete, consider removing it from the external DNS to prevent it from becoming a potential security risk in the future.

Example Analysis:

- **Unresolved Subdomain:** `legacyservice.demodata.com`
  - **Status:** Unresolved
  - **Action:** Monitor for reactivation. If this subdomain becomes resolvable again, ensure that it is properly secured or decommissioned if it is no longer needed.
- **Offline Subdomain:** `api.demo2.demodata.com`
  - **Resolved IP:** 172.16.0.2
  - **Status:** Offline (could not be probed)
  - **Analysis:** This subdomain resolves to an IP address but is not reachable, possibly due to firewall protection or server downtime. Review the necessity of this subdomain being externally resolvable. If it is not required for external use, consider removing it from DNS to reduce the attack surface.

Importance of Monitoring Inactive Subdomains:

Inactive subdomains, whether unresolved or offline, can pose a hidden threat. Attackers may exploit these subdomains if they become active again without proper security controls. Regular monitoring and periodic review of inactive subdomains help ensure that they do not inadvertently become vulnerabilities within your organization's digital infrastructure.

Understanding SSL/TLS Information Results

The SSL/TLS Information section provides a detailed overview of the SSL/TLS certificates used by the subdomains of the scanned domain. SSL/TLS certificates are crucial for securing data transmitted between a user's browser and the server, ensuring data integrity, confidentiality, and authenticity. The scan results include key information such as the SSL grade, certificate issuer, version of SSL/TLS in use, and expiration dates. This information helps assess the security posture of the domain and identify areas that may need improvement.

Overview of SSL/TLS Information:

This section lists each subdomain with details about its SSL/TLS configuration:

1. **SUBDOMAIN URL:**
   The URL of the subdomain using SSL/TLS, such as `https://portal.demodata.com`. This URL indicates the specific subdomain for which the SSL/TLS certificate is being evaluated.
2. **SSL GRADE:**
   A grade indicating the quality of the SSL/TLS configuration for the subdomain. Grades typically range from A+ (excellent) to F (poor), with considerations such as encryption strength, supported protocols, and presence of security vulnerabilities.
3. **ISSUED BY:**
   Information about the Certificate Authority (CA) that issued the SSL/TLS certificate. This includes the common name (CN) and organization (O) of the issuer, such as "Let's Encrypt" or "DigiCert Inc." Reputable CAs enhance the trustworthiness of the certificate.
4. **ISSUED TO:**
   Details about the entity to which the certificate was issued. This includes the common name (CN) and, if applicable, the organization (O) that owns the certificate. The common name usually matches the domain name, indicating that the certificate is valid for that specific subdomain.
5. **SELF SIGNED?:**
   Indicates whether the certificate is self-signed (`YES`) or issued by a trusted Certificate Authority (`NO`). Self-signed certificates are less secure because they are not validated by a trusted third party and may be vulnerable to man-in-the-middle attacks.
6. **VERSION NAME:**
   Specifies the version of SSL/TLS in use, such as `TLSv1.2` or `TLSv1.3`. Newer versions (e.g., TLSv1.3) offer improved security features and should be preferred over older versions, which may have known vulnerabilities.

7. **EXPIRATION TIME (UTC):**
   The date and time when the SSL/TLS certificate will expire. An expired certificate can result in security warnings in users' browsers and may expose the subdomain to potential security risks. It's important to renew certificates before they expire to maintain secure communication.

Example Analysis:

Here are some example analyses based on the SSL/TLS scan results:

- **Subdomain:** `https://rdp.demodata.com`
  - **SSL Grade:** A+
  - **Issued By:** Let's Encrypt
  - **Issued To:** `rdp.demodata.com`
  - **Self Signed?:** NO
  - **Version Name:** TLSv1.3
  - **Expiration Time:** 11/04/2023, 06:49 AM
  - **Analysis:** This subdomain has an excellent SSL grade (A+), indicating a secure SSL/TLS configuration. The certificate is issued by a reputable CA (Let's Encrypt) and supports TLSv1.3, the latest version with enhanced security features. The certificate is not self-signed and is valid until April 2023, ensuring secure communication for the subdomain.
- **Subdomain:** `https://soc.demodata.com`
  - **SSL Grade:** T
  - **Issued By:** COMODO CA Limited
  - **Issued To:** `*.oversig.ht`
  - **Self Signed?:** NO
  - **Version Name:** TLSv1.2
  - **Expiration Time:** 18/04/2019, 11:59 PM
  - **Analysis:** This subdomain has a low SSL grade (T), which indicates potential issues with its SSL/TLS configuration. The certificate is outdated, having expired in April 2019, which can lead to browser security warnings and expose the subdomain to security risks. Additionally, the certificate was issued for `*.oversig.ht` rather than the subdomain itself, suggesting a possible misconfiguration. Immediate action is required to renew the certificate and ensure it matches the subdomain correctly.
- **Subdomain:** `https://webconf.demodata.com`
  - **SSL Grade:** B
  - **Issued By:** DigiCert Inc
  - **Issued To:** `*.demodata.com`
  - **Self Signed?:** NO
  - **Version Name:** TLSv1.2
  - **Expiration Time:** 30/11/2023, 11:59 PM
  - **Analysis:** This subdomain has a moderate SSL grade (B), indicating a decent but not perfect SSL/TLS setup. The certificate is issued by a reputable CA (DigiCert Inc) and

is valid until November 2023. However, it uses TLSv1.2, which, while secure, can be updated to TLSv1.3 for enhanced security. Some improvements may be needed to achieve a higher grade, such as reviewing the supported ciphers and protocols.

Importance of SSL/TLS Monitoring:

Regularly monitoring SSL/TLS configurations is crucial to maintaining a secure environment. Properly configured SSL/TLS certificates ensure encrypted data transmission, protect against man-in-the-middle attacks, and provide users with confidence when accessing your services. Identifying and addressing issues such as expired certificates, outdated protocols, or weak encryption is key to strengthening the overall security posture of your domain.