EyeQ Dot Net Pvt. Ltd.

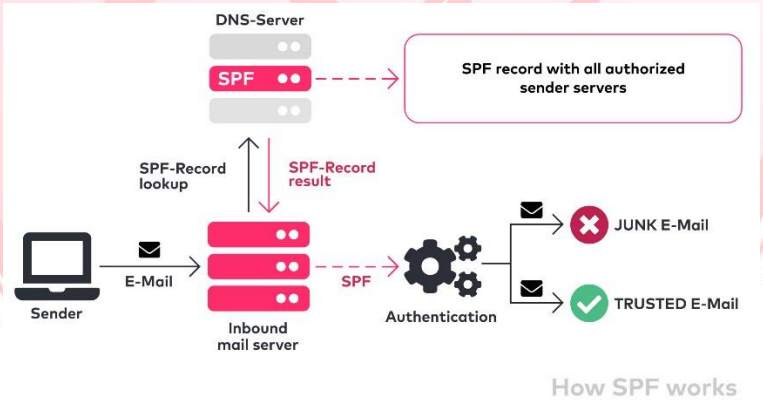
LEARN FROM REAL HACKERS

TASK 7: SPF RECORD

What is a SPF Record?

A Sender Policy Framework (SPF) record is a DNS record that specifies which IP addresses or servers are authorized to send emails on behalf of a particular domain. By defining these trusted sources, SPF helps prevent email spoofing and phishing by enabling email servers to verify whether incoming emails from a domain are legitimate. SPF records enhance email security by reducing the chances of fraudulent or malicious emails being accepted by recipients' servers.

How does an SPF work?



How SPF works

An SPF (Sender Policy Framework) record works by allowing domain owners to list authorized mail servers that can send emails on behalf of their domain. Here's how it works in practice:

1. **SPF Record Setup:** The domain owner creates an SPF record in the domain's DNS settings. This record is a type of TXT entry that includes a list of IP addresses or hostnames authorized to send emails for the domain.

2. **Email Verification**: When an email server receives an incoming message claiming to be from the domain, it performs a DNS lookup to retrieve the SPF record associated with the sender's domain.

3. **Matching IP Addresses:** The receiving server compares the IP address of the sending server against the list of IPs in the SPF record. If the IP is listed, the email passes SPF verification.

4. **Pass, Fail, or Soft Fail**: Based on the match, the SPF check will either pass (valid sender), fail (unauthorized sender), or result in a soft fail (warning but not rejection). The receiving server can then use this information to determine whether to accept, flag, or reject the email.

Why should a company add SPF Record to their domain?

Adding an SPF (Sender Policy Framework) record to a company's domain is essential for improving email security and protecting brand integrity. Here's why:

1. **Prevents Email Spoofing:** By specifying which servers are authorized to send emails for the domain, SPF reduces the risk of unauthorized senders pretending to be the company, which is crucial in preventing email-based fraud, phishing, and impersonation attacks.

2. **Protects Brand Reputation:** A compromised email reputation due to spoofed messages can harm a company's brand. SPF helps ensure that only legitimate emails reach recipients, helping maintain trust and credibility with clients and partners.

3. **Improves Email Deliverability:** Many email servers check SPF records before delivering messages. Emails from domains without an SPF record are more likely to be marked as spam or blocked. With an SPF record, emails are more likely to reach the intended inbox, improving communication reliability.

4. **Supports Compliance and Security Standards:** Many cybersecurity frameworks recommend SPF as a best practice for securing email. Adding SPF helps a company align with email security standards, enhancing its overall security posture.

How do companies implement an SPF Record on their domain?

To implement an SPF record, companies follow a series of steps to define authorized email senders for their domain in the DNS settings:

1. **Identify Authorized Mail Servers:** First, the company determines all servers, IP addresses, or third-party services (e.g., marketing or CRM platforms) authorized to send emails for their domain.

2. **Create the SPF Record:** Using the gathered information, the company constructs an SPF record as a TXT entry. The format typically begins with `v=spf1`, followed by the IP addresses or hostnames of authorized servers, and ends with a rule (e.g., `-all` to specify that only listed servers are permitted).

Example SPF record:

- **v=spf1**: This tells the server that the record contains an SPF record
- **v=spf1 a include: spf.google.com ~all**: This record authorizes Google Workspace to send emails for your domain
- **v=spf1 include:spf.protection.outlook.com -all**: This is an example of an SPF record for a Microsoft 365 domain

3. **Add the SPF Record to DNS:** The company logs into their domain registrar or DNS management portal and adds the SPF record as a TXT entry in the DNS settings. This entry links to the domain and specifies the authorized servers.

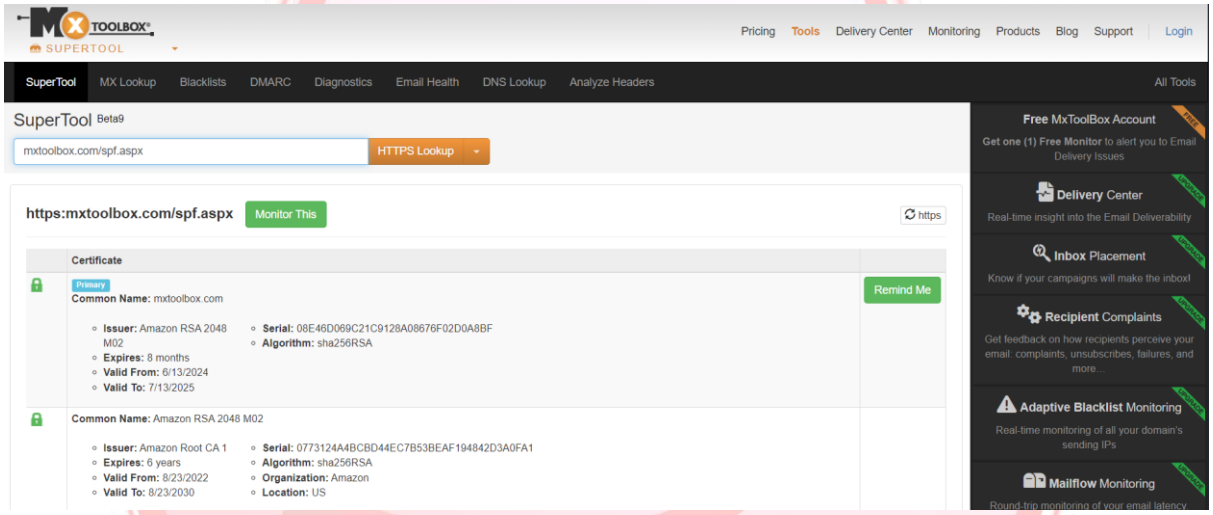
4. **Test the SPF Record:** After publishing the record, the company can verify its effectiveness with SPF validation tools. These tools simulate email checks to ensure the SPF record is configured correctly and that emails from authorized servers are successfully validated.

5. **Monitor and Adjust as Needed:** Over time, the company should monitor email delivery and adjust the SPF record if they add new email services or retire old ones to keep the record accurate and effective.

How to check the missing SPF Record bug?

To check for a missing SPF record bug, which indicates that a domain lacks an SPF entry or that an existing entry is not functioning correctly, follow these steps:

1. **Use Online SPF Checkers:** Online SPF validation tools, such as MXToolbox, SPF Record Checker, or Google Admin Toolbox, allow users to verify if an SPF record is present and correctly configured. Enter the domain name, and the tool will display any SPF records found or report if none exist.



2. **DNS Lookup:** Perform a DNS TXT record lookup using command-line tools like **nslookup**, **dig**, or **host**. Running a command like **nslookup -type=TXT example.com** (replacing **example.com** with the actual domain) will display any TXT records, including SPF, if configured. If no SPF record is returned, the domain lacks SPF protection.

3. **Check Email Headers:** If you have received an email from the domain, examine its headers by selecting "Show Original" (or equivalent) in your email client. Look for "Received-SPF" or similar information, which shows whether an SPF check was performed. A "none" result suggests an SPF record is missing or misconfigured.

4. **Review Error Messages:** Some email servers provide diagnostic messages or warnings if an SPF record is missing. These messages often appear in email bounce-back notifications or email logs and may advise on SPF configuration.

References:

https://www.cloudflare.com/learning/dns/dns-records/dns-spf-record/

https://mxtoolbox.com/spf.aspx