S.No	Problem Statement ID	Problem Statement Name	Domain
8	CT-AICS - 04	DNS Spoofing / Email Spoofing detection tool	AI Cyber Sec

Description :

The **DNS Spoofing / Email Spoofing Detection Tool** is designed to help individuals and organizations detect and prevent spoofing attacks.

- **DNS Spoofing**: A cyberattack where attackers redirect users from legitimate websites to malicious ones by altering the DNS (Domain Name System) records.
- **Email Spoofing**: A tactic where attackers forge the sender's email address to make it appear as if the email came from a trusted source, often used for phishing or spreading malware.

This tool will monitor and identify suspicious activities in DNS records or email headers, helping users detect and mitigate spoofing attempts.

Objectives :

1. **Detect DNS Spoofing:**
    - Monitor DNS records for unauthorized changes.
    - Identify mismatched or suspicious IP addresses that do not correspond to legitimate servers.
2. **Identify Email Spoofing:**
    - Analyze email headers to detect forged sender addresses.
    - Check for discrepancies in SPF, DKIM, and DMARC records.
3. **Prevent Spoofing Damage:**
    - Alert users about spoofing attempts in real-time.
    - Provide actionable steps to secure DNS settings or block malicious emails.
4. **Educate Users:**
    - Teach users to recognize the signs of DNS and email spoofing attacks.

Expectations :

1. **For Developers:**
   - Create a tool that scans DNS records and email headers for anomalies.
   - Use automation to provide real-time alerts for potential spoofing activities.
2. **For Users:**
   - Offer a user-friendly interface for analyzing DNS settings and email security.
   - Provide detailed reports and recommendations to mitigate risks.
3. **For Organizations:**
   - Enable businesses to protect their domain and email infrastructure from spoofing attacks.
   - Improve email deliverability and reduce the risk of phishing or reputation damage.

Expected Results :

1. **Timely Detection:**
   - Quickly identify DNS or email spoofing attempts before they cause harm.
2. **Improved Security:**
   - Protect users from phishing, malware, and data theft by securing DNS and email systems.
3. **Actionable Recommendations:**
   - Provide clear steps to fix vulnerabilities and prevent future attacks.
4. **Increased Awareness:**
   - Educate users about DNS and email spoofing tactics, helping them stay vigilant.