# **CTF Topic: Suspicious Email Header Analytics**

# **Introduction**



In this CTF challenge, you will analyze the header of a suspicious email to identify potential red flags and extract critical information such as the source IP, location, threat level, and hostname. Email headers contain essential metadata about the email's path, sender, and recipient, which can help you detect phishing attempts, spoofing, and other malicious activities.

# **Tools and requirements**

* [DNSchecker web app toolkit](https://dnschecker.org/email-header-analyzer.php)

# **Scenario**



You have received an email that appears to be from a trusted source, but something about it seems off. Your task is to analyze the email header to determine if the email is legitimate or if it poses a potential threat. By examining the email header, you will extract key information such as the source IP, location, threat level, and hostname.

# **Process to Perform**

First Download the Email Header File From Step 1 and analyze it through the DNSCHecker web application tool kit given on Step 2.

Step 1: Download the email Header File: [Click Here](https://www.mediafire.com/file/kee850ae0btx7s8/Email.eml/file)

Step 2: After downloading, open it with notepad and copy all the data open [DNSchecker web app toolkit](https://dnschecker.org/email-header-analyzer.php) this link and paste it

# **Let's Begin The Challenge**

# **Question**

Flag1: What is the Source IP address of Email?

Answer: 149.72.214.208

Flag Captured

Flag 2: Find Out Host Name?

Answer: o28.ck.m.convertkit.com.

Flag Captured

Flag 3: What is the level of Threat?

Answer: low

Flag Captured

Flag 4: What is the Zip Code?

Answer:80202

Flag Captured

# **Hint**

