Network System security

Assignment-3 Report

Submitted By

Anjali Singh

M.Tech Cyber Security

2023JCS2565

Submitted To

Mr. Vireshwar Kumar

Indian Institute Of Technology, Delhi

1 Sending Email

1.1 Sending from Gmail to IITD-mail

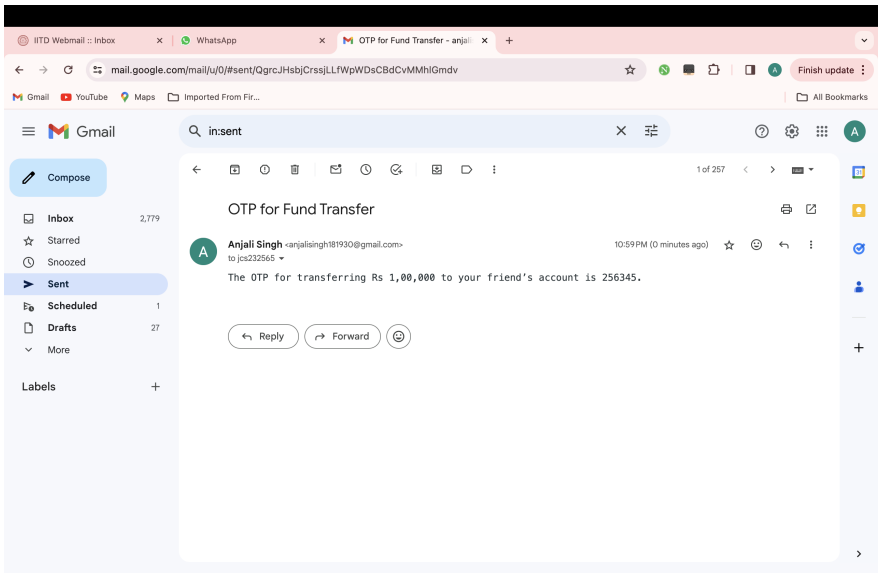

Figure 1: Sending email to iitd from gmail account manually

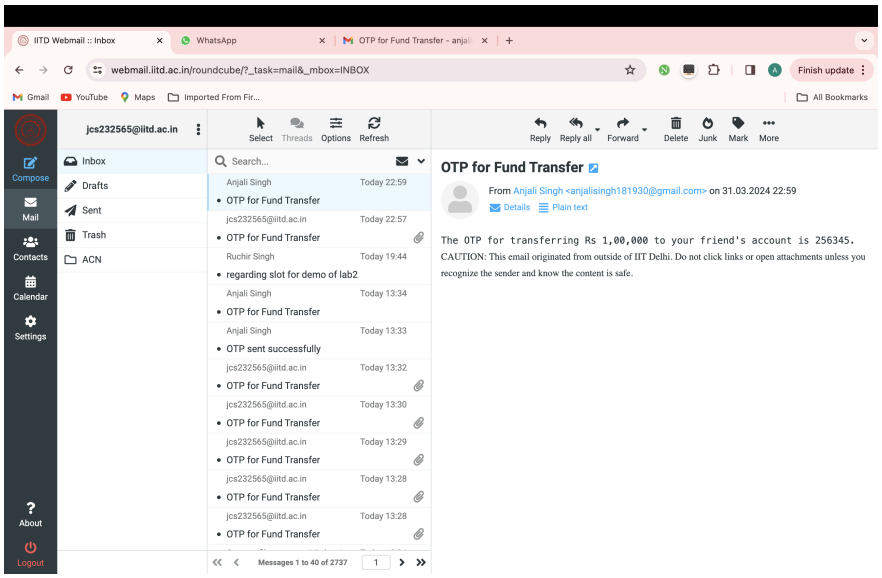

Figure 2: Mail recieved in IITD inbox

1.2 Sending from IITD-mail to IITD-mail

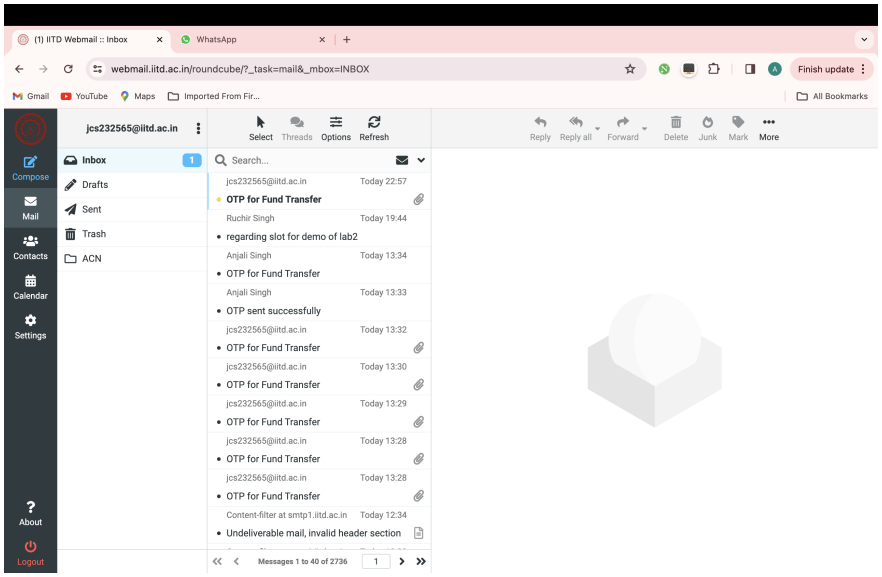

Figure 3: Sending email to iitd mail using python script

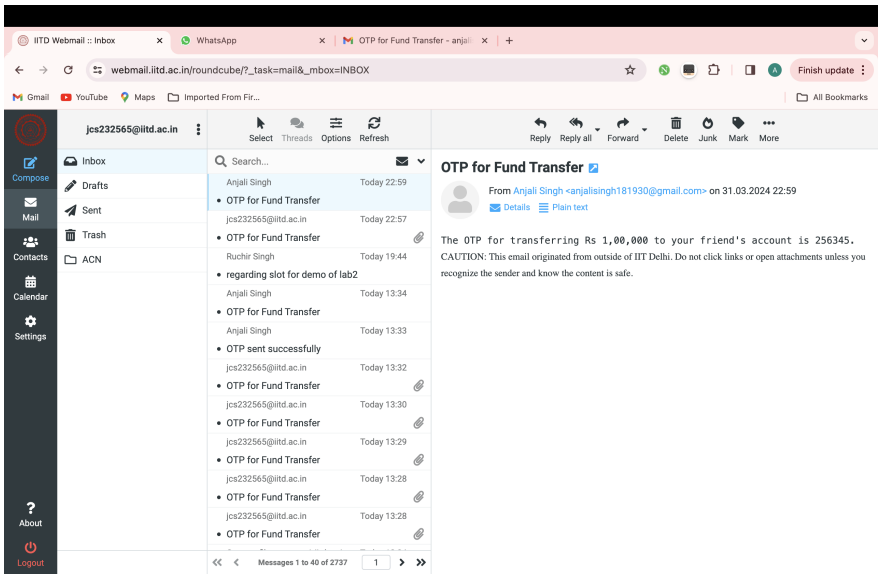

Figure 4: Mail recieved in IITD inbox

2 Receiving Email

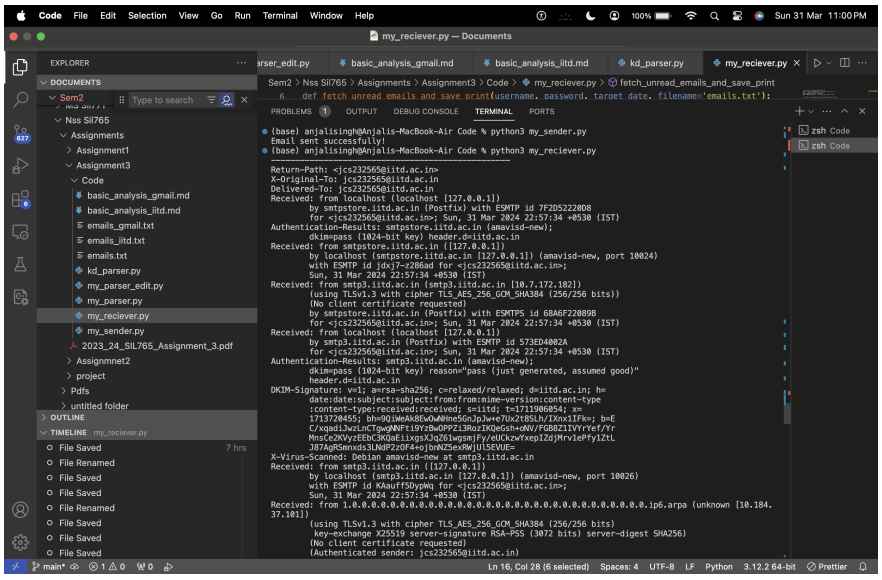

Figure 5: Email retrieved from iitd webmail inbox using python script

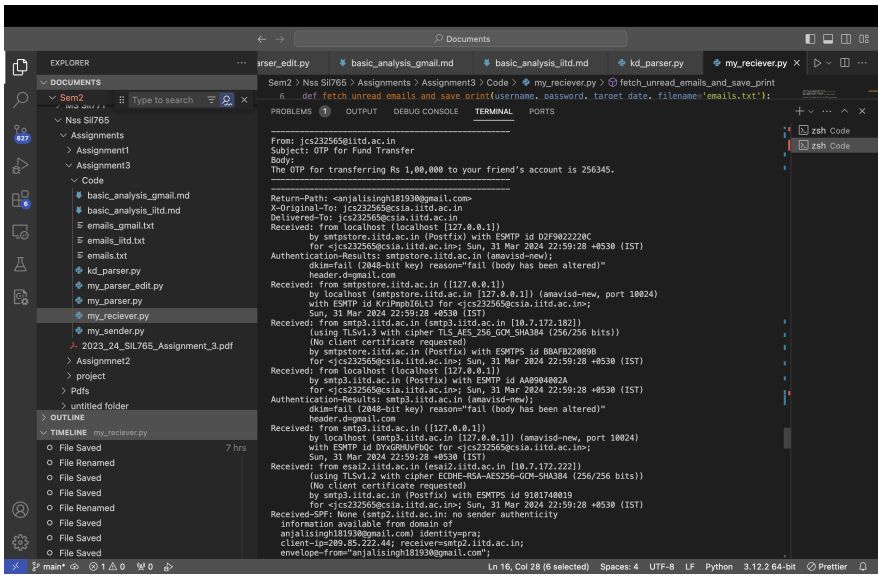

Figure 6: Email retrieved from iitd webmail inbox using python script

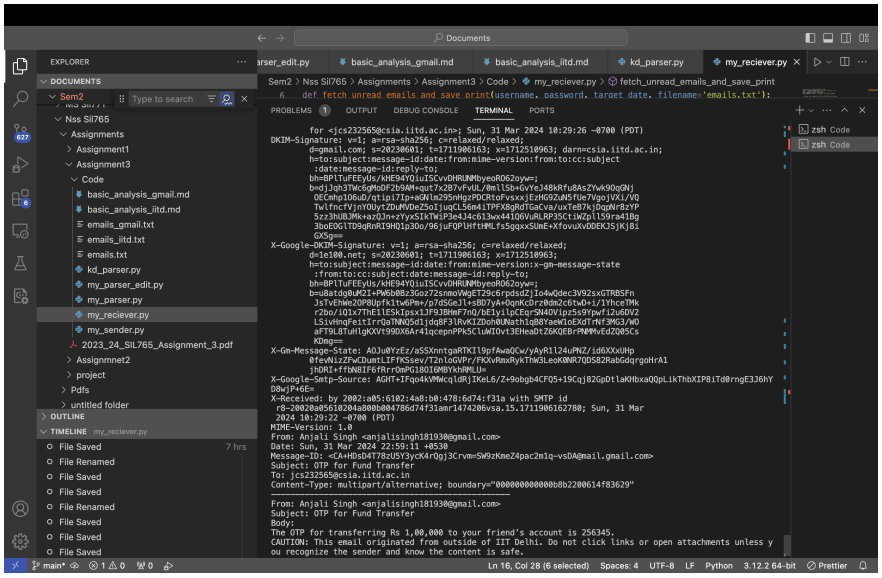

Figure 7: Email retrieved from iitd webmail inbox using python script

3 Parsing Headers of both Mails

3.1 Parsing Header of mail sent from Gmail to IITD-mail

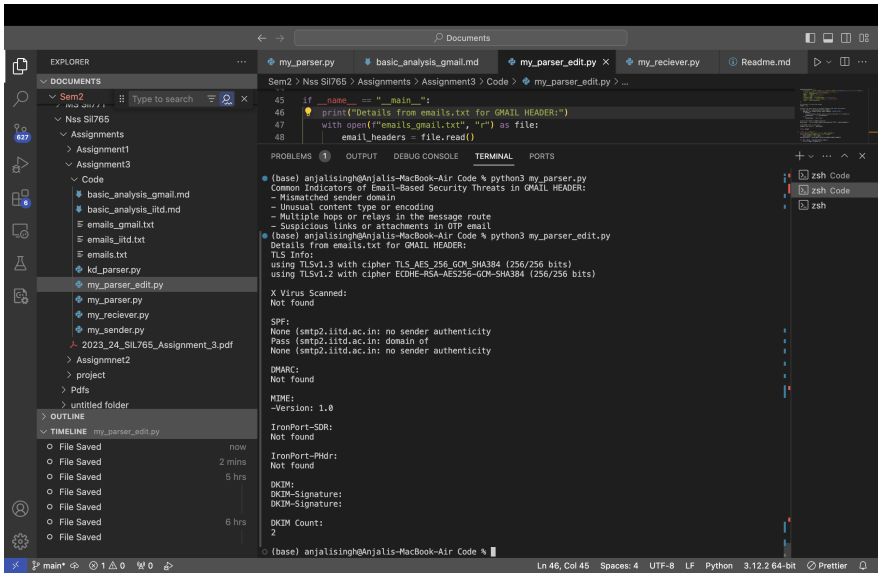

Figure 8: Mail sent from Gmail to IITD-mail Header Parsed

3.2 Parsing Header of mail sent from IITD-mail to IITD-mail

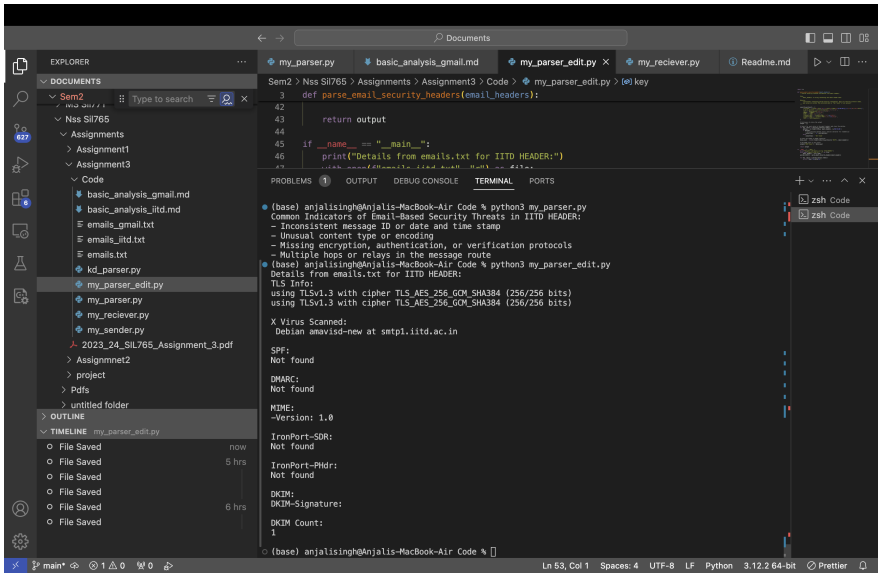

Figure 9: Mail sent from IITD-mail to IITD-mail Header Parsed

4 Basic Analysis

4.1 For Mail sent from IITD-mail to IITD-mail

- **TLSv1.3:** This is a secure transport layer protocol used to encrypt the email content during transmission between mail servers. It's a good sign and helps protect against eavesdropping attempts.

- **DKIM (DomainKeys Identified Mail):** This is an email authentication protocol that helps verify the sender's domain. It can help prevent email spoofing to some extent.

  [label=**Effectiveness against Attacks:**]**TLSv1.3:** While TLSv1.3 is a robust protocol, it's not foolproof. Theoretically, a Man-in-the-Middle attack with sufficient resources could potentially exploit vulnerabilities in the implementation. However, such attacks are complex and less likely for internal email communication within a trusted network like IITD. **DKIM:** DKIM can prevent basic email

spoofing attempts where someone sends an email pretending to be from another address. However, it has limitations:

- – It doesn't verify the sender's identity, only the domain. A malicious user with access to an authorized account within the domain (e.g., compromised IITD account) could still send emails with a valid DKIM signature.
  – DKIM relies on the receiving mail server to check the DKIM signatures, and some less secure mail servers might not implement this check.

[label=**Missing Protocols:**]**SPF (Sender Policy Framework):** This protocol complements DKIM by specifying authorized mail servers for a domain. It can help further prevent spoofing attacks. **DMARC (Domain-based Message Authentication, Reporting & Conformance):** This builds on SPF and DKIM and allows domain owners to instruct receiving mail servers on how to handle unauthenticated emails. It can be a valuable tool for identifying and mitigating email spoofing attempts.

Overall Security: The use of TLSv1.3 and DKIM provides a baseline level of security for IITD emails. However, for enhanced protection against sophisticated attacks, implementing SPF and DMARC would be recommended.

4.2 Mail sent from Gmail to IITD-mail

- **Header Information:**
  – The email header provides metadata about the email, including routing information, timestamps, and authentication results.
- **Return-Path:**
  – The Return-Path field specifies the email address to which bounce messages are sent in case of delivery issues.
- **X-Original-To:**
  – X-Original-To indicates the original recipient of the email.

- **Received:**
  - This field shows the journey of the email through various mail servers. Each Received field represents a point in the transmission path, showing the server that received the email, along with timestamps and server information.
- **Authentication Results:**
  - This section provides details about the email authentication process, including SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting, and Conformance) results.
  - SPF is used to verify that the sending server is authorized to send emails on behalf of the domain.
  - DKIM involves digitally signing emails to verify that they haven't been altered in transit.
  - DMARC specifies how email receivers should handle emails that fail SPF or DKIM checks.
- **IronPort-SDR and IronPort-PHdr:**
  - These fields contain additional information related to email processing and security checks performed by IronPort, which is a brand of email security appliances.
- **X-IPAS-Result:**
  - This field likely contains the result of a spam filtering or security analysis performed by an email security product, possibly related to Cisco's IronPort.
- **Analysis:**
  - The email failed DKIM verification, indicating that the email's body had been altered after being signed. This could be due to legitimate modifications by intermediate mail servers or malicious tampering.

- SPF and DMARC checks passed, indicating that the email originated from an authorized server for the specified domain and that the domain has a DMARC policy in place, which wasn't strict enough to reject the email outright.
- The IronPort-SDR and IronPort-PHdr sections suggest that additional security checks were performed by Cisco IronPort appliances, likely including spam filtering and malware detection.

5 Advanced Analysis

Step-by-Step Methodology to Authenticate the DKIM Signature in the Email:

1. **Header Information:**
   - Review the email header to locate the DKIM-Signature field.
2. **DKIM (DomainKeys Identified Mail):**
   - Extract the DKIM-Signature field from the email header.
   - Retrieve the public DKIM key associated with the sender's domain.
   - Decode the DKIM-Signature field to extract relevant information.
3. **Public Key Retrieval:**
   - Use DNS resolution to fetch the public DKIM key.
4. **Signature Verification:**
   - Compute a new cryptographic hash of the email body.
   - Decrypt the digital signature using the sender's public DKIM key.
   - Compare the computed hash with the hash extracted from the DKIM-Signature field.
5. **Result Interpretation:**
   - If the hashes match, the DKIM signature is valid.

6. **Overall Assessment:**

    - Evaluate the DKIM authentication results along with other email security protocols.

6 Comparative Analysis

IITD MHS Security Features:

- **Security Protocols:**
  - TLSv1.3: Secure transport layer protocol used for encryption.
  - DKIM: Email authentication protocol to verify sender's domain.
- **Effectiveness against Attacks:**
  - TLSv1.3: Provides encryption but vulnerable to sophisticated attacks.
  - DKIM: Prevents basic email spoofing but has limitations regarding sender identity verification.
- **Missing Protocols:**
  - SPF: Absent, would complement DKIM for preventing spoofing attacks.
  - DMARC: Absent, would enhance email authentication and handling.
- **Overall Security:**
  - TLSv1.3 and DKIM provide baseline security, but implementing SPF and DMARC is recommended for enhanced protection.

DKIM Signature Verification for IITD MHS:

[leftmargin=1cm]**DKIM Signature:**

- – **Status:** Passed
  - **Domain:** iitd.ac.in

Authentication Results for IITD MHS:

[leftmargin=1cm]**Authentication-Results:**

- – **Status:** Passed
  - – **Method:** DKIM
  - – **Domain:** iitd.ac.in

Received Information for IITD MHS:

[leftmargin=1cm]**Received:**

- – **From:** smtp1.iitd.ac.in
  - – **Protocol:** TLSv1.3
  - – **Cipher:** TLS_AES_256_GCM_SHA384
  - – **Authentication:** Authenticated sender

GMAIL Security Features:

- **Security Protocols:**
  - – TLSv1.3: Secure transport layer protocol used for encryption.
  - – DKIM: Email authentication protocol to verify sender's domain.
- **Effectiveness against Attacks:**
  - – TLSv1.3: Provides encryption but vulnerable to sophisticated attacks.
  - – DKIM: Prevents basic email spoofing but has limitations regarding sender identity verification.
- **Missing Protocols:**
  - – SPF: None found, absence could lead to spoofing vulnerabilities.
  - – DMARC: None found, absence may result in inadequate email authentication and handling.

- **Overall Security:**
  - Similar to IITD MHS, Gmail could benefit from implementing SPF and DMARC for enhanced security.

DKIM Signature Verification for GMAIL:

[leftmargin=1cm]**DKIM Signature:**

- **Status:** Failed
- **Domain:** gmail.com

Authentication Results for GMAIL:

[leftmargin=1cm]**Authentication-Results:**

- **Status:** Passed
- **Method:** SPF
- **Domain:** gmail.com

Received Information for GMAIL:

[leftmargin=1cm]**Received:**

- **From:** esai2.iitd.ac.in
- **Protocol:** TLSv1.2
- **Cipher:** ECDHE-RSA-AES256-GCM-SHA384
- **Authentication:** None