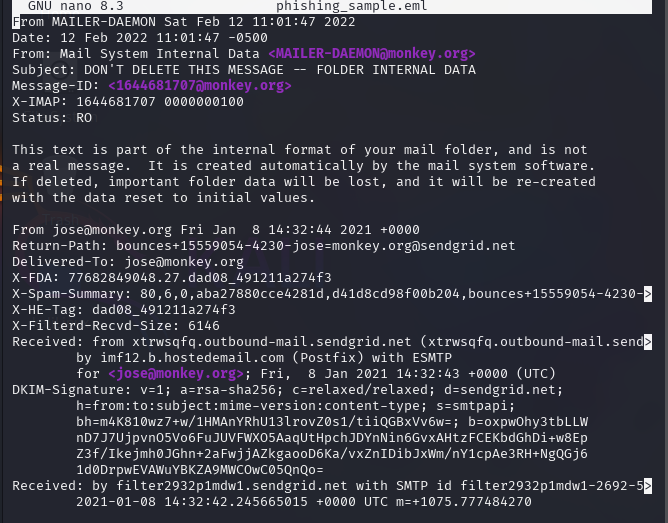
**ANALYZE A PHISHING EMAIL SAMPLE**



1 Snapshot of phishing email

**HEADER FIELD ANALYSING:**

1. From: Mail System Internal Data [MAILER-DAEMON@monkey.org](mailto:MAILER-DAEMON@monkey.org)
2. Return-Path: [bounces+15559054-4230-jose=monkey.org@sendgrid.net](mailto:bounces+15559054-4230-jose=monkey.org@sendgrid.net) (It should have matched **FROM:** but since it did not match so it might be a spoofed one)

* The Return-Path uses SendGrid (a legit email service), but the From: claims to be [jose@monkey.org](mailto:jose@monkey.org).
* If monkey.org doesn’t use SendGrid, this is a spoofing attempt.

1. Received: from xtrwsqfg.outbound-mail.sendgrid.net ... by infl2.b.hostedemail.com

* sendgrid.net doesn’t align with sender’s domain monkey.org.
* The email is relayed through a suspicious server

1. DKIM-Signature: v=1; a=rsa-sha256; d=sendgrid.net; ...

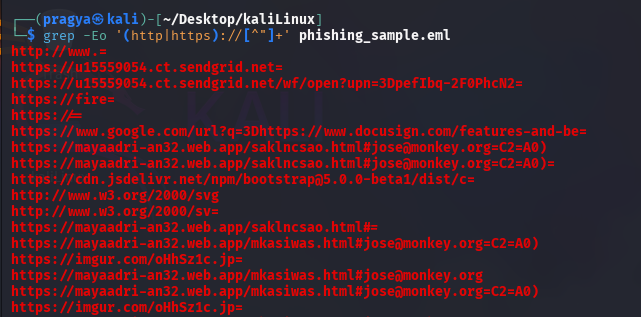
* D=sendergrid.net which doesn’t match sender’s domain monkey.org
* Mismatching shows spoofing likely

1. X-Spam-Summary: 80,6,0,aba27880cce4281d,d4d8cd98f00b204,...

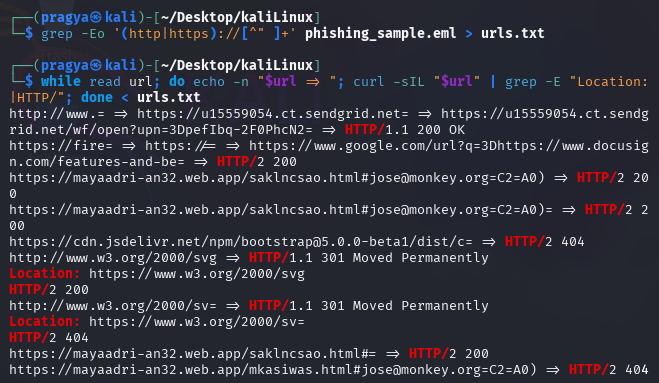
* 80 is a high spam score (0-100 scale)
* Phishing indicator : legit emails rarely score > 50

**Inspecting Links & Attachments:**

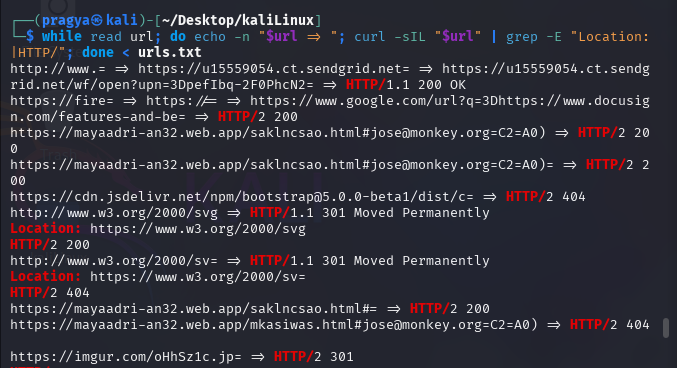
Identifying suspicious links



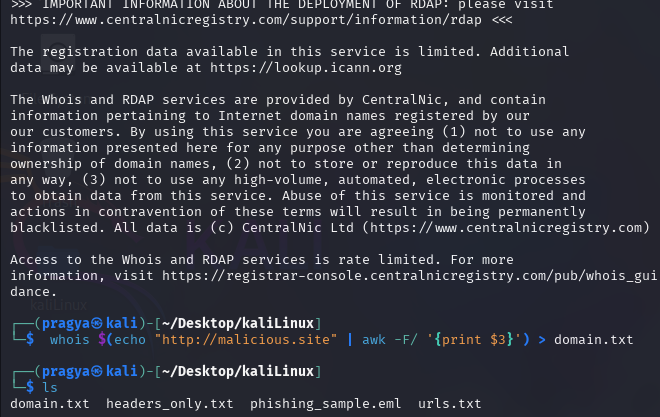
2 Snapshot of some URLs extracted from the email



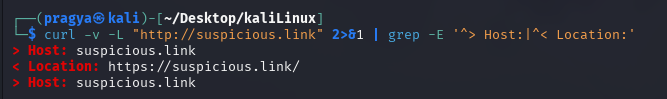
3 Saved all the URLs to a text file and doing automated analysis



4 Checking redirects and headers

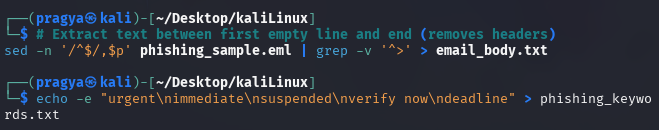


5 Domain age check

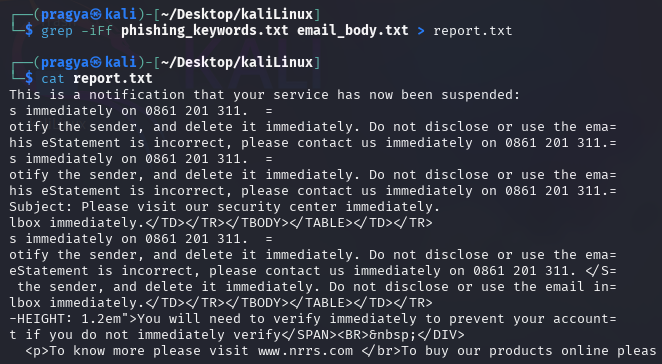
Checking for redirects:

6 Tracing redirects

Looking for urgent or threatening language in email body:



7 Automated Keyword Analysis



8 Scanned report

**RESULT:**

After analysis, we confirm the scanned email is a phishing attempt. Key indicators include urgent language and spoofed sender addresses.

**CONCLUSION:**

Analysed a phishing mail and understood about phishing tactics and learnt email threat analysis skills