Task 2: Analyze a Phishing Email Sample.

PHISHING EMAIL ANALYSIS USING KALI LINUX

Prerequisites

- Kali Linux installed (bare metal, VM, or WSL)
- Sample phishing email (preferably .eml, .msg, or full raw content)
- Optional: Internet access for online tools

View Full Email Source

```
cat phishing-email.eml
```

Or open in a text editor:

```
nano phishing-email.eml
```

Analyze Email Headers

```
sudo apt install libemail-outlook-message-perl
```

To Run:

```
exiftool phishing-email.eml
```

Or use header analyzer websites (safe):

https://toolbox.googleapps.com/apps/messageheader/

https://mxtoolbox.com/EmailHeaders.aspx

Look for:

Sender IP

SPF/DKIM/DMARC results

Time stamps mismatch

Decode Base64 / Encoded Data

Phishing emails often contain encoded payloads

```
grep -i 'base64' -A 20 phishing-email.eml > encoded.txt
base64 -d encoded.txt > decoded.html
```

Review the HTML for fake login forms or scripts:

```
cat decoded.html
```

Extract URLs

```
grep -Eo '(http|https)://[^"]+' phishing-email.eml
```

```
sudo apt install urlscan
urlscan phishing-email.eml
```

Inspect URLs Safely

```
whois malicious-url.com
dig malicious-url.com
```

Examine Attachments

```
munpack phishing-email.eml
```

If it’s a Word/Excel doc, use:

```
oleid sample.doc
olevba sample.doc
```

Look for macros or shell commands.

For PDFs:

```
pdfid.py file.pdf
pdf-parser.py file.pdf
```

Analyze HTML Payloads

```
cat decoded.html
```

Use Public Repositories of Phishing Emails

Download it:

```
git clone https://github.com/mitchellkrogza/Phishing.Database.git
cd Phishing.Database
```

View the Full Email

```
cat phishing-sample.eml
```

Identify Key Header Fields

```
From: "PayPal Support" <support@security-paypa1.com>
Reply-To: support@scammer.com
Return-Path: <bounce@phishhost.com>
Received: from unknown ([203.0.113.45])
```

Identify Suspicious Links or Attachments in a Phishing Email

Open the Email File

```
cat phishing-sample.eml
```

Extract and Inspect All Links

```
grep -Eo '(http|https)://     ' phishing-sample.eml
grep -aEo '(http|https)://[a-zA-Z0-9./?=_-]*' phishing-sample.eml
```

Hover vs Actual Link (in HTML)

```
<a href="http://phishy-login.ru">https://www.paypal.com/secure</a>
```

Look for Attachments

```
grep -i "Content-Disposition" phishing-sample.eml
```

Analyze the Attachment (if extracted)

```
file Invoice_8327.pdf
strings Invoice_8327.pdf | less
exiftool Invoice_8327.pdf
```

To decode a base64 file:

```
base64 -d suspicious_payload.b64 > decoded_payload
```

Use URL Reputation Tools (Optional but Recommended)

Paste any suspicious links into:

VirusTotal

urlscan.io

PhishTank

Look for Urgent or Threatening Language in the Email Body

How to Do It (Manually or via Kali Linux)

```
cat phishing-sample.eml | less
```

You can also extract just the body:

```
grep -A 50 -i "Content-Type: text/html" phishing-sample.eml
```

Example Email Body Snippet:

```
<p>Dear user,</p>

<p>We have detected suspicious activity on your account. If you do not verify your identity within the next 24 hours, your account will be permanently suspended.</p>

<p><a href="http://secure-login-update.com">Click here to verify now</a></p>
```

Analysis:

- **"suspicious activity"** = fear tactic
- **"within the next 24 hours"** = urgency
- **"permanently suspended"** = threat
- **"Click here to verify"** = call to action leading to phishing page

Note Any Mismatched URLs (Hover to See Real Links)

How It Works

<a href="http://malicious-site.ru/secure-login">https://www.paypal.com/secure</a>

Search for <a href=... HTML tags

```
grep -i '<a href' phishing-sample.eml
```

Manually Compare the Anchor Text and Actual Link

<a href="http://login.paypalsecure.ru">https://www.paypal.com/secure</a>

What Actions Should Be Taken on Suspected Phishing Emails

DO NOT:

- Do not click on any links or buttons
- Do not open any attachments
- Do not reply to the sender
- Do not forward the email to others casually

Disconnect from the Internet (If You Clicked Something Suspicious)

. Report the Phishing Email

Delete or Quarantine the Email

Check for Compromise (If Interacted with Email)

How Attackers Use **Social Engineering** in Phishing

Phishing is **not just a technical attack** — it's a **psychological one**. Social engineering is the **manipulation of human behavior** to trick victims into doing what the attacker wants (like clicking a malicious link or giving up credentials).

What Is Social Engineering in Phishing?

Social engineering in phishing uses deception, urgency, and impersonation to make you:

- Click unsafe links
- Open malicious attachments
- Enter personal or financial information
- Download malware
- Transfer money

Social engineering techniques used:

- **Fear** ("Your account has been locked")
- **Urgency** ("Verify within 24 hours")
- **Impersonation** (Fake PayPal link)
- **Authority** (Uses brand and tone of a security team)

How to Protect Yourself

- Always **pause and verify** suspicious emails
- Never trust **urgency or emotional pressure**
- **Don't click links** in emails — type URLs manually
- Use **multi-factor authentication (MFA)**
- Train employees and yourself with **phishing simulations**

Consultation

Cybersecurity Consultation: Phishing & Threat Detection

Phishing remains one of the most prevalent and dangerous cyber threats targeting individuals and organizations alike. It is often the entry point for larger attacks such as data breaches, ransomware infections, or credential theft. A comprehensive understanding of email spoofing, social engineering, header analysis, and detection practices is essential for defense.

Phishing and Social Engineering

Phishing attacks rely heavily on social engineering — the psychological manipulation of users to bypass technical defenses. These emails are carefully crafted to create a sense of urgency, fear, or authority, prompting recipients to click malicious links, download attachments, or share confidential information.

Common tactics include impersonation of trusted entities (e.g., banks, IT departments, executives), emotional triggers ("Your account will be suspended"), and convincing-looking web pages that steal credentials. Training users to identify these manipulations is a critical first line of defense.

Email Spoofing & Header Analysis

Phishing campaigns often use email spoofing to disguise the sender's identity. This is typically done by forging the From: address to appear as if the email comes from a trusted source. To detect spoofing and analyze potential phishing emails, it's essential to examine the email headers, which contain routing information.

Header analysis involves checking:

- The From:, Reply-To:, and Return-Path: fields for mismatches.
- The Received: lines to trace the actual origin of the message.
- Authentication results such as SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC

- (Domain-based Message Authentication, Reporting & Conformance) to verify if the email passed sender validation.

Forensic analysis tools and header analyzers can quickly identify inconsistencies and help determine whether a message is genuine or malicious**.**

Threat Detection and Mitigation

Effective threat detection requires both technical controls and human awareness. On the technical side, deploying secure email gateways with phishing and malware detection, URL and attachment sandboxing, and threat intelligence feeds is crucial. Additionally, implementing strict SPF, DKIM, and DMARC policies can reduce the likelihood of successful spoofing.

From a user perspective, ongoing security awareness training and simulated phishing campaigns are key to building resilience. Users should be encouraged to report suspicious emails and know how to spot red flags such as mismatched URLs (where the link text doesn't match the real destination), poor grammar, unexpected attachments, or requests for credentials.

In the event of a suspected phishing incident, organizations should follow an incident response plan that includes:

- Isolating affected systems
- Resetting compromised credentials
- Scanning endpoints for malware
- Reviewing logs and email headers
- Notifying relevant stakeholders or authorities if necessary