Phishing Analysis Tools

# 📘 Phishing Analysis Tools – Notes

### **Task 1 – Introduction**

* Phishing is one of the most common cyber attack techniques.
* Objective: Learn to analyze phishing emails, extract IOCs, and verify legitimacy.

### **Task 2 – What information should we collect?**

When analyzing a suspicious email, always collect:

* **Email header** (sender, recipient, timestamps, SPF/DKIM/DMARC results).
* **Email body** (content, URLs, attachments).
* **Attachments** (check file type, hashes, sandbox).
* **URLs/domains** (check for redirection, reputation, SSL certs).

### **Task 3 – Email header analysis**

* Reveals **metadata** of the email.
* Important fields:
  + From: vs. Return-Path: (spoofing signs).
  + Received: chain (origin IP, mail server path).
  + Message-ID: (check domain legitimacy).
  + SPF/DKIM/DMARC results.
* Tools: MXToolbox, MessageHeader Analyzer.

### **Task 4 – Email body analysis**

* Look for:
  + **Suspicious links** (hover before clicking).
  + **Obfuscation** (hidden HTML, base64 text, homoglyphs).
  + **Urgency or scare tactics** ("Your account will be locked").
* Extract and check URLs using VirusTotal, URLScan.io.

### **Task 5 – Malware Sandbox**

* Attachments are often malicious payloads (Office macros, executables, PDFs).
* Safe way: Upload to sandbox (Any.Run, Hybrid Analysis, Joe Sandbox).
* Look for network behavior, file system changes, registry changes.
* Collect IOCs (IPs, domains, hashes).

### **Task 6 – PhishTool**

* Specialized tool for phishing investigation.
* Features:
  + Automated email header analysis.
  + Detects spoofing, phishing attempts.
  + Highlights malicious indicators.

### **Task 7 – Phishing Case 1**

* Example of analyzing a suspicious email.
* Steps:
  + Check **header authenticity**.
  + Identify **suspicious domains**.
  + Verify links with VirusTotal/URLScan.
  + Conclusion: Malicious.

### **Task 8 – Phishing Case 2**

* Different email sample (e.g., fake invoice/payment).
* Attachment analysis in sandbox reveals malware behavior.
* Extracted IOCs → confirm phishing attempt.

### **Task 9 – Phishing Case 3**

* Another scenario (credential harvesting).
* Body analysis shows fake login page.
* URLs linked to **typosquatted domains**.
* Confirm phishing through reputation check.

### **Task 10 – Conclusion**

* Key process in phishing analysis:
  1. Collect header, body, attachment, URLs.
  2. Analyze headers for spoofing.
  3. Inspect body for malicious intent.
  4. Sandbox test attachments.
  5. Use tools (PhishTool, URLScan, VirusTotal).
  6. Document & share IOCs.

