Phishing Analysis Fundamentals

## **Intro to Malware Analysis – Notes**

### **Task 1 – Introduction**

* Malware Analysis = process of examining malicious software to understand:
  + Functionality
  + Origin
  + Impact
  + How to detect & defend against it
* Used in **DFIR, threat intelligence, SOCs, and reverse engineering**.

### **Task 2 – Malware Analysis**

* Goals:
  + Identify indicators of compromise (IOCs)
  + Understand malware’s persistence & execution methods
  + Support detection & prevention strategies
* Key outputs:
  + Hashes, domains, IPs, registry keys, processes, artifacts.

### **Task 3 – Techniques of Malware Analysis**

1. **Static Analysis** (without execution)
   * File hashing, string extraction, PE header inspection, libraries & imports.
2. **Dynamic Analysis** (run malware in sandbox/VM)
   * Observe network activity, processes, persistence, dropped files.
3. **Advanced Analysis (Reverse Engineering)**
   * Debugging, disassembly (IDA, Ghidra, x64dbg).
   * Used for deep inspection of malware logic.

### **Task 4 – Basic Static Analysis**

* Quick, safe, first step.
* Tools: strings, PEiD, Detect-It-Easy, VirusTotal, YARA.
* Look for:
  + Hardcoded IPs/domains
  + API calls
  + Encryption keys
* Pros: Fast, safe.
* Cons: Limited if obfuscation/packing is used.

### **Task 5 – The PE File Header**

* Windows executables follow **Portable Executable (PE)** format.
* Contains metadata about program:
  + **DOS Header** → legacy MS-DOS info.
  + **PE Header** → info about architecture, entry point.
  + **Sections** → .text, .data, .rdata, .rsrc.
  + **Imports/Exports** → functions from DLLs.
* Malware analysts use PE header to identify how a file runs and its dependencies.

### **Task 6 – Basic Dynamic Analysis**

* Run malware in **controlled environment (sandbox, VM)**.
* Monitor:
  + **Processes** → Process Hacker, Procmon
  + **Registry changes** → Regshot
  + **Network traffic** → Wireshark, Fakenet-NG
  + **File system changes** → Process Monitor, Sysinternals tools
* Provides **behavioral indicators**.

### **Task 7 – Anti-analysis techniques**

* Malware often uses **evasion techniques**:
  + **Packing/Obfuscation** → UPX, custom packers
  + **Anti-debugging** → timing checks, debugger detection
  + **Anti-VM checks** → looking for VirtualBox, VMware artifacts
  + **Code injection** → RunPE, hollowing into benign processes
  + **Encryption** → hides strings & payloads

### **Task 8 – Conclusion**

* Malware analysis helps defenders:
  + Extract IOCs
  + Improve detections (YARA/Sigma rules)
  + Understand adversary TTPs
* Balanced approach = static + dynamic + advanced analysis.

