Tempest

# 🌀 Tempest — Notes

### **Task 1: Introduction**

* DFIR-style lab simulating a real intrusion.
* Covers attacker techniques: initial access, persistence, privilege escalation, and objectives.
* Blue team role: analyze logs, traffic, and artifacts.

### **Task 2: Preparation – Log Analysis**

* Start with **Windows Event Logs** & **Sysmon logs**.
* Look for unusual process execution, PowerShell commands, or suspicious parent/child processes.
* Correlate timestamps across logs.

### **Task 3: Preparation – Tools and Artifacts**

* Tools used:
  + **Event Viewer / Wevtutil / Get-WinEvent** → log review.
  + **Sysinternals (Procmon, Autoruns, TCPView)**.
  + **Wireshark / Zeek logs** → network traffic.
  + **Sigma rules** for threat detection.
* Artifacts: Prefetch, Registry keys, Scheduled tasks, Services.

### **Task 4: Initial Access – Malicious Document**

* Delivery method: malicious document (likely Word with macros).
* Execution triggered a dropper payload.
* Indicators: suspicious file in **Downloads/Desktop**, abnormal process spawn (winword.exe → powershell.exe).

### **Task 5: Initial Access – Stage 2 Execution**

* Malicious document downloaded **second-stage payload**.
* Network connections to external IP/domain.
* Dropped and executed malware (DLL/EXE).
* Persistence may be established via registry run key or scheduled task.

### **Task 6: Initial Access – Malicious Document Traffic**

* Network logs reveal:
  + **HTTP traffic** to C2.
  + Suspicious domains (e.g., newly registered).
  + Possible **base64/encoded PowerShell** in requests.
* Identify attacker C2 IP and domain.

### **Task 7: Discovery – Internal Reconnaissance**

* Attacker ran reconnaissance commands:
  + whoami, ipconfig /all, net user /domain, net group /domain.
* Collected domain info, users, and systems.
* Goal: map internal environment.

### **Task 8: Privilege Escalation – Exploiting Privileges**

* Attacker exploited privilege escalation (vulnerable service or misconfig).
* Techniques:
  + Token impersonation.
  + Abuse of SeDebugPrivilege.
  + UAC bypass.
* End result: gained SYSTEM/Admin rights.

### **Task 9: Actions on Objective – Fully-owned Machine**

* Final attacker objectives:
  + **Exfiltration** of sensitive files.
  + Possible **backdoor installation** for persistence.
  + Machine fully compromised.
* Blue team takeaway:
  + Trace IOCs (hashes, IPs, domains).
  + Harden logging & detection.
  + Patch privilege escalation vector.

