Redline

## **Redline – Notes**

### **Task 1 – Introduction**

* Redline is a **free endpoint forensics tool** developed by **FireEye (Mandiant)**.
* Used for **memory analysis** and **host investigation**.
* Supports:
  + Memory captures (RAM dumps).
  + File system and registry analysis.
  + IOC (Indicators of Compromise) searches.
* Useful in DFIR to analyze malware, persistence, and attacker activity.

### **Task 2 – Data Collection**

* Redline uses **Collectors** to gather data from endpoints.
* Two main types of collectors:
  1. **Standard Collector** – Collects a wide range of system data (processes, services, drivers, registry, file system, etc.).
  2. **IOC Search Collector** – Collects system data and searches for **indicators of compromise** (hashes, domains, filenames).
* Output: Collection results are saved in a **.mans file** for analysis in Redline.

### **Task 3 – The Redline Interface**

* Main interface components:
  + **Overview Tab** – High-level system summary.
  + **Timeline Tab** – Displays execution and file activity chronologically.
  + **Processes Tab** – Running processes, hierarchy, and details.
  + **Files Tab** – File system data.
  + **Registry Tab** – Registry keys and values.
  + **Network Tab** – Network connections, listening ports, etc.
* Allows pivoting between artifacts to correlate evidence.

### **Task 4 – Standard Collector Analysis**

* Provides full **host-based forensic data**.
* Key artifacts:
  + **Processes** → Suspicious parent/child relationships.
  + **Services/Drivers** → Malicious persistence.
  + **Registry Keys** → Autoruns, startup entries.
  + **File System** → Recently modified or unusual files.
* Helps detect anomalies like **suspicious executables, unsigned drivers, persistence mechanisms**.

### **Task 5 – IOC Search Collector**

* IOC = **Indicator of Compromise** (hashes, filenames, domains, IPs).
* Redline allows importing **IOC definitions** in .ioc format.
* Collector searches the system for matches against IOC sets.
* Efficient for **targeted threat hunting** (e.g., searching for known malware hash).

### **Task 6 – IOC Search Collector Analysis**

* After collection, Redline displays a list of **matches**.
* Analysts review IOC hits and validate if they are **benign or malicious**.
* Example:
  + IOC match on **MD5 hash** of a file → check its path, signer, reputation.
  + IOC match on **domain name** → verify if it is a known C2 server.
* Redline highlights potential **malware or persistence evidence**.

### **Task 7 – Endpoint Investigation**

* Analysts use Redline to:
  + **Investigate processes**: Check parent-child hierarchy (e.g., explorer.exe spawning cmd.exe).
  + **Check autoruns/persistence**: Registry Run keys, scheduled tasks.
  + **Analyze memory artifacts**: DLL injections, hidden processes.
  + **Review network activity**: Outbound connections to suspicious IPs.
* Useful for **root cause analysis** and **attribution**.

### **Task 8 – Conclusion**

* Redline is a **powerful free DFIR tool** for memory and endpoint forensic analysis.
* Key strengths:
  + Timeline reconstruction.
  + IOC-based hunting.
  + Detailed system investigation.
* Limitations:
  + Requires manual analysis skills.
  + Can miss advanced fileless malware.
* Commonly used in **SOC investigations, malware analysis, and IR workflows**.

