NetworkMiner

## 🕵️‍♂️ **NetworkMiner – TryHackMe Room Notes**

### ✅ **Task 1: Room Introduction**

* **Objective:** Learn how to use NetworkMiner to extract and analyze artifacts from PCAP files.
* NetworkMiner is a passive network sniffer/packet analyzer widely used in **network forensics**.
* Capable of reconstructing files, sessions, and metadata from packet captures.

### ✅ **Task 2: NetworkMiner in Forensics**

* In network forensics, NetworkMiner helps:
  + Extract **usernames, passwords**, and **downloaded files**.
  + Reconstruct entire communication sessions.
  + Identify **malicious activity** in compromised systems.
* **Benefits:**
  + Operates passively (doesn’t send packets).
  + Can analyze large PCAPs quickly and intuitively.

### ✅ **Task 3: What is NetworkMiner?**

* Developed by **Erik Hjelmvik**.
* Functions:
  + Parses **PCAP/PCAPNG files**.
  + Extracts:
    - **Hosts**
    - **Sessions**
    - **Credentials**
    - **Files**
    - **DNS queries**
* Runs on **Windows**, can be used via **Mono** on Linux.

### ✅ **Task 4: Tool Overview 1**

#### Tabs in NetworkMiner:

* **Hosts Tab:**
  + Lists IPs and MAC addresses.
  + OS fingerprinting and hostname detection.
* **Files Tab:**
  + Shows reconstructed files transferred in sessions.
  + Can export files directly for further analysis.
* **Images Tab:**
  + Reconstructs images transferred (e.g., in HTTP).

### ✅ **Task 5: Tool Overview 2**

* **Credentials Tab:**
  + Displays credentials (HTTP basic auth, FTP, POP3, etc.).
* **Parameters Tab:**
  + HTTP GET/POST parameters.
  + Helps detect **sensitive data leakage**.
* **Messages Tab:**
  + Reconstructs chat/email messages if available.
* **Sessions Tab:**
  + Full list of TCP sessions for inspection.

### ✅ **Task 6: Version Differences**

* **Free vs. Professional:**
  + Free version is powerful enough for most educational and forensic purposes.
  + Pro includes:
    - Live sniffing.
    - GeoIP mapping.
    - Command line scripting.
    - Plugin support.

### ✅ **Task 7: Exercises**

🔍 Practice analyzing a provided PCAP file using NetworkMiner:

* Find:
  + List of communicating hosts.
  + Extracted files/images.
  + Any exposed credentials.
  + Sessions containing suspicious activity.
* Pay attention to:
  + User-Agent strings.
  + Domains/IPs contacted.
  + Unusual ports or protocols.

### ✅ **Task 8: Conclusion**

* **NetworkMiner** is a powerful and easy-to-use tool for **PCAP analysis** and **network forensics**.
* Especially helpful in SOC, DFIR, and threat hunting roles.
* Use it to quickly extract IOCs and evidence from packet captures.

## 🛠️ Tips for Effective Use:

* Use NetworkMiner alongside tools like **Wireshark** for deeper packet-level inspection.
* Always verify file hashes and metadata when analyzing suspicious file transfers.
* Check **DNS**, **Credentials**, and **Sessions** tabs thoroughly for early signs of compromise.

