Velociraptor

# Velociraptor – Notes

### **Task 1: Introduction**

* Velociraptor = endpoint visibility & digital forensics tool.
* Open-source, used for DFIR and threat hunting.
* Client-server model → server deploys, client agents collect data.
* Key features: live forensics, fast hunting, custom queries with **VQL**.

### **Task 2: Deployment**

* Runs on **Windows, Linux, macOS**.
* Setup includes:
  + Velociraptor server (management, storage).
  + Clients (agents on endpoints).
* Config via velociraptor config generate.
* Supports standalone deployment for single investigations.

### **Task 3: Interacting with Client Machines**

* Interaction via:
  + **GUI (Web interface)**
  + **Command line**
* Provides system overview: processes, network, registry, files.
* Can run custom collections (investigation tasks) on clients.

### **Task 4: Creating a New Collection**

* **Collections** = tasks to gather forensic data.
* Can collect artifacts like:
  + Event logs
  + Prefetch files
  + Browser history
  + Network connections
* Use prebuilt or custom artifacts (YAML-based).

### **Task 5: VFS (Virtual File System)**

* Provides a **file-system-like view** of client machines.
* Allows browsing:
  + Files
  + Registry hives
  + System directories
* Analysts can **download suspicious files** for offline analysis.

### **Task 6: VQL (Velociraptor Query Language)**

* SQL-like query language.
* Used to define artifacts and hunts.
* Examples:
  + SELECT \* FROM pslist() → running processes.
  + SELECT \* FROM netstat() → network connections.
* Flexible for filtering, hunting, and data extraction.

### **Task 7: Forensic Analysis VQL Plugins**

* Velociraptor ships with built-in plugins for:
  + **Process analysis** → pslist, pstree
  + **Network analysis** → netstat, dns
  + **Registry analysis** → reg\_key, userassist
  + **File system analysis** → file, mft
* Plugins extend Velociraptor’s forensic capabilities.

### **Task 8: Hunt for a Nightmare**

* **Hunts** = run queries across multiple endpoints at scale.
* Used for:
  + Detecting persistence mechanisms
  + Searching for malware artifacts
  + Identifying suspicious processes / registry keys
* "Hunt for a nightmare" = wide-scale threat hunting scenario.

### **Task 9: Conclusion**

* Velociraptor = powerful DFIR tool for enterprise-scale incident response.
* Combines:
  + Endpoint monitoring
  + Data collection
  + Threat hunting
  + Memory & disk forensics
* Key strengths: speed, scalability, and customization with VQL.

