Velociraptor

Threat Hunting Tool

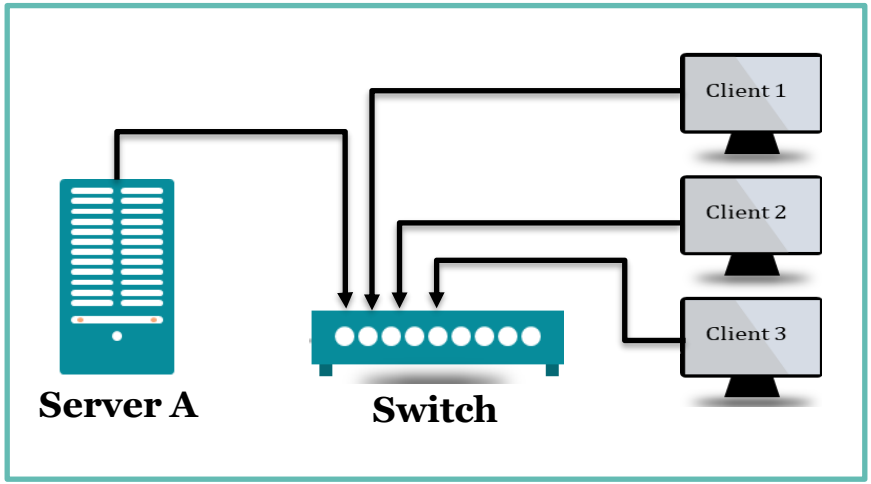
What is Velociraptor

Velociraptor is an advanced digital forensic and incident response tool that enhances your visibility into your endpoints.

Velociraptor is a tool for collecting host based state information using The Velociraptor Query Language (VQL) queries.

- Hunt for evidence of sophisticated adversaries
- Investigate malware outbreaks and other suspicious network activities
- Monitory continuously for suspicious user activities, such as files copied to USB devices
- Discover whether disclosure of confidential information occurred outside the network
- Gather endpoint data over time for use in threat hunting and future investigations

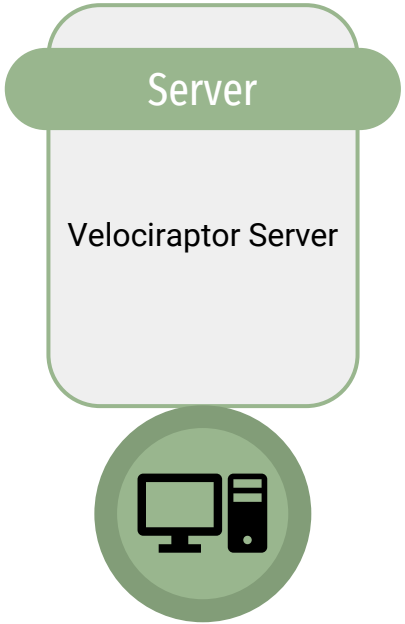
Deployment



Need to Acknowledge

- Before Installation:
  System must communicate with each other
  Test – Ping <IP>
- During Installation:
  Read installation steps carefully
  Provide Ips required by the environment
- Post Installation
  Long lasting system connectivity

Velociraptor Model



Pre-Requisites

- Cmd/PowerShell with admin access
- All systems must communicate with each other and must be in same network

Velociraptor Server Installation

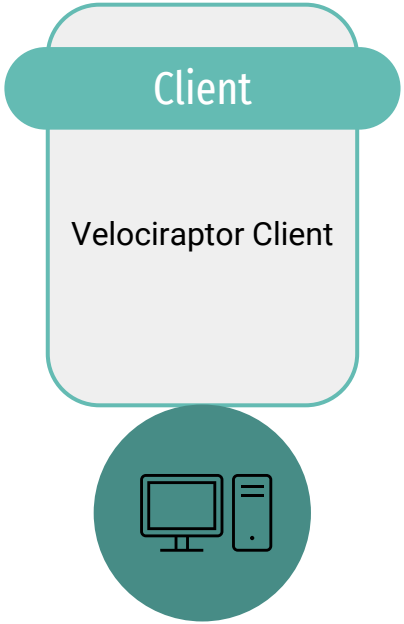
- Download Repo - https://github.com/Velocidex/velociraptor
- ./velociraptor.exe config generate –l
- ./velociraptor.exe - -config server.config.yaml user add admin - -role administrator
- ./velociraptor.exe - -config server.config.yaml frontend -v

Velociraptor Client Installation

- ./velociraptor.exe - -config client.config.yaml client –v

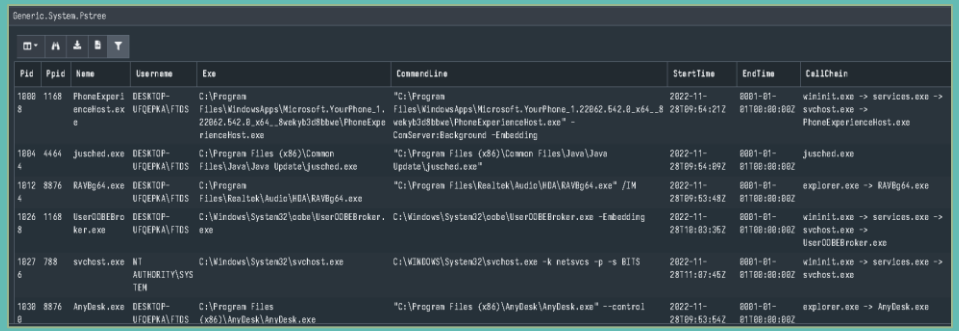
Key Points

- Always mention host IP in place of localhost, if clients are other systems
- Always copy same exe and other files on client which are generated during server installation



Velociraptor Basic Required Artifacts List

- *Windows.Network.listeningPorts*
- *Windows.System.Pslist*
- *Generic.System.Pstree*
- *Windows.EventLogs.RDPAuth*
- *Windows.KapeFiles.Targets*
- *EvidenceOFExecution/UserAssist*
- *Generic.Forensic.LocalHashes.Glob*
- *Windows.Attack.ParentProcess*
- *Windows.Attack.Prefetch*
- *Windows.Attack.UnexpectedImagePath*
- *Windows.Applications.TeamViewer.Incoming*
- *Windows.Forensics.Shellbags*
- *Windows.System.Services*



Pros & Cons

- Can not generate alerts
- Same network dependency

- Can hunt the system using inbuilt feature as well as manual commands
- Simple Deployment
- No High Capacity of hardware required

Thank You