

Velociraptor

Threat Hunting Tool



What is Velociraptor

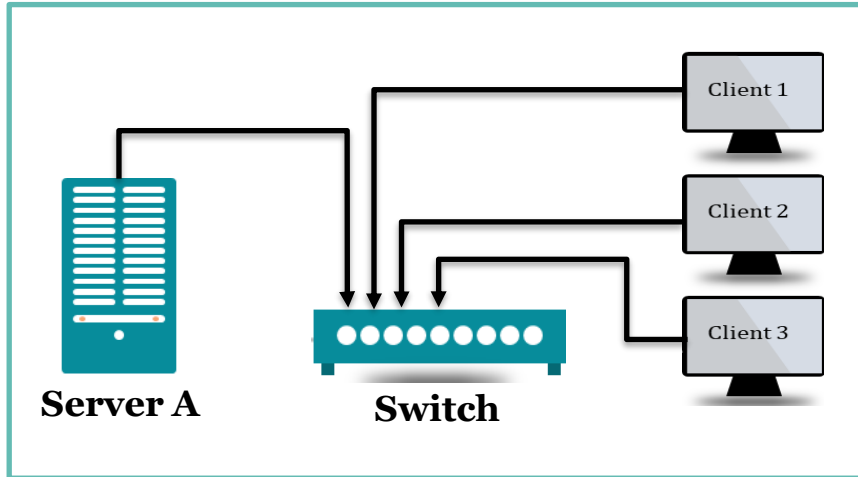


Velociraptor is an advanced digital forensic and incident response tool that enhances your visibility into your endpoints.

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
- Monitor 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

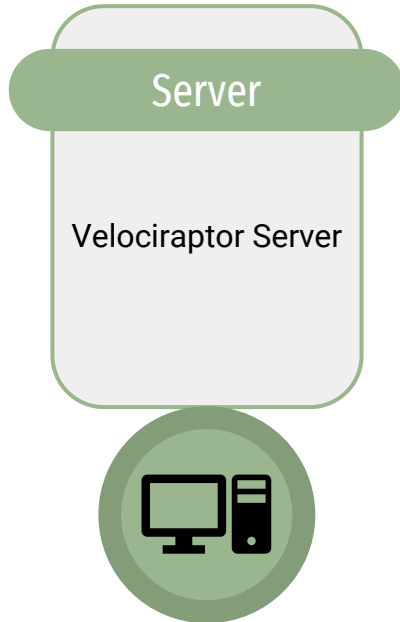
Deployment



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

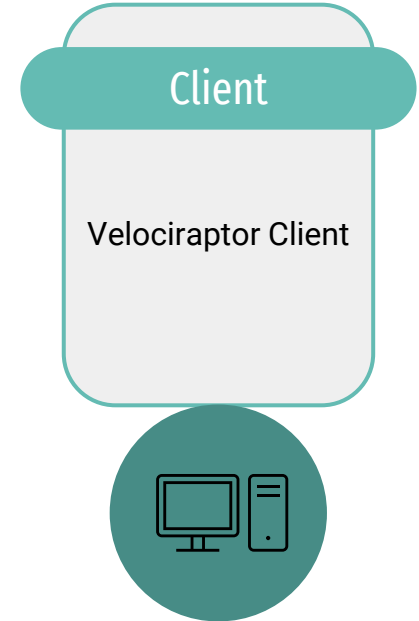
- Download Repo - <https://github.com/Velocidex/velociraptor>
- `./velociraptor.exe config generate -l`
- `./velociraptor.exe -config server.config.yaml user add admin -role administrator`
- `./velociraptor.exe -config server.config.yaml frontend -v`

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*

Generic.System.Pstree

Pid	Ppid	Name	Username	Exe	CommandLine	StartTime	EndTime	CallChain
1800	1168	PhoneExperiencelost.exe	DESKTOP-UFGPKA\FDOS	C:\Program Files\WindowsApps\Microsoft.YourPhone.1.22062.642.0_x-ww_8-wk9b3c8bbe\PhoneExperienceHost.exe	"C:\Program Files\WindowsApps\Microsoft.YourPhone.1.22062.642.0_x-ww_8-wk9b3c8bbe\PhoneExperienceHost.exe" - CoSrvr:Background -Embedding	2022-11-28T09:54:21Z	0001-01-01T00:00:00Z	wininit.exe -> services.exe -> svchost.exe -> PhoneExperienceHost.exe
1804	4464	jusched.exe	DESKTOP-UFGPKA\FDOS	C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe	"C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe"	2022-11-28T09:54:09Z	0001-01-01T00:00:00Z	jusched.exe
1812	8876	RAVBg64.exe	DESKTOP-UFGPKA\FDOS	C:\Program Files\Realtek\Audio\HDA\RAVBg64.exe	"C:\Program Files\Realtek\Audio\HDA\RAVBg64.exe" /IM	2022-11-28T09:53:49Z	0001-01-01T00:00:00Z	explorer.exe -> RAVBg64.exe
1826	1168	UserOOBEBroker.exe	DESKTOP-UFGPKA\FDOS	C:\Windows\System32\oobe\UserOOBEBroker.exe	C:\Windows\System32\oobe\UserOOBEBroker.exe -Embedding	2022-11-28T10:03:56Z	0001-01-01T00:00:00Z	wininit.exe -> services.exe -> UserOOBEBroker.exe
1827	788	svchost.exe	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe	C:\WINDOWS\System32\svchost.exe -k netsvcs -p -s BITS	2022-11-28T11:07:46Z	0001-01-01T00:00:00Z	wininit.exe -> services.exe -> svchost.exe
1830	8876	AnyDesk.exe	DESKTOP-UFGPKA\FDOS	C:\Program Files (x86)\AnyDesk\AnyDesk.exe	"C:\Program Files (x86)\AnyDesk\AnyDesk.exe" --control	2022-11-28T09:53:54Z	0001-01-01T00:00:00Z	explorer.exe -> AnyDesk.exe

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

