**ANALYZING MEMORY WITH VOLATILITY**

**Walkthrough: Using Volatility for Memory Analysis**

1. **Updating and Installing Python 2**:

🡪 **sudo apt update**

**sudo apt install python2**

* + Updates the package lists and installs Python 2, which is required for Volatility 2.

A screen shot of a computer

AI-generated content may be incorrect.A screenshot of a computer program

AI-generated content may be incorrect.

1. **Installing Development Tools**:

**🡪 sudo apt install build-essential python2-dev gcc g++ make**

* + Installs essential tools and libraries required to build Python dependencies.

A screenshot of a computer program

AI-generated content may be incorrect.

1. **Installing Python Packages**:
   * Commands to install required Python packages:

**🡪 python2 -m pip install distorm3==3.3.4**

**python2 -m pip install pycryptodome==3.4.7**

**python2 -m pip install yara-python==3.11.0**

**python2 -m pip install -r requirements.txt**

**sudo apt-get update**

**sudo apt-get install python2.7**

**sude apt-get install python-pip**

**sudo apt-get install python-dev**

**sudo apt-get install libpcap-dev**

* + These are dependencies needed for Volatility to analyze memory dumps.

A computer screen shot of a program

AI-generated content may be incorrect.A computer screen shot of a program code

AI-generated content may be incorrect.

A computer screen shot of a program code

AI-generated content may be incorrect.A screenshot of a computer program

AI-generated content may be incorrect.

1. **Installing Volatility**:

**🡪 sudo apt-get install python-volatility**

* + Installs Volatility 2.6.1 from the package manager.
  + Check that all file in the volatility directory with (**LS**)

A computer screen shot of a computer code

AI-generated content may be incorrect.

A screen shot of a computer

AI-generated content may be incorrect.

**Using Volatility**

1. **Checking Available Profiles**:

**🡪 python2 vol.py**

* + Lists the supported profiles for analyzing memory dumps.

A screenshot of a computer

AI-generated content may be incorrect.

1. **Analyzing a Memory Image**:
   * Identifying the image profile:

**🡪 python2 vol.py -f /home/$(whoami)/volatility/zeus2x4.mem imageinfo**

* + - imageinfo: Detects the most suitable profile for the memory image.
  + Example output includes profile suggestions like WinXP SP2x86.

A screen shot of a computer

AI-generated content may be incorrect.

1. **Running Analysis Plugins**:
   * **Listing Processes**:

**🡪 python2 vol.py -f /home/$(whoami)/volatility/zeus2x4.vmem -- profile=WinXP SP2x86 pslist**

* + - pslist: Lists active processes in the memory dump.A screenshot of a computer screen

      AI-generated content may be incorrect.
  + **Malware Analysis**:

🡪 **python2 vol.py -f /home/$(whoami)/volatility/zeus2x4.vmem -- profile=WinXP SP2x86 malfind**

* + - malfind: Detects potential malware in the memory image.

A computer screen shot of a computer code

AI-generated content may be incorrect.

* + **Network Connections**:

🡪 ( I use connscan because netscan doesn’t support the profile )

A screen shot of a computer program

AI-generated content may be incorrect.

**🡪 python2 vol.py -f /home/$(whoami)/volatility/zeus2x4.vmem --profile=WinXP SP2x86 connscan**

* + - connscan: Scans for active network connections.

A screen shot of a computer

AI-generated content may be incorrect.

* + **Listing DLLs**:

**🡪 python2 vol.py -f /home/$(whoami)/volatility/zeus2x4.mem --profile=WinXP SP2x86 dlllist**

* + - dlllist: Lists loaded DLLs for all processes.

A computer screen shot of a program

AI-generated content may be incorrect.

THANK YOU