CSE 5472: Memory Forensics Lab

Objective

Learn about performing memory forensics on compromised systems.

Deliverable

1. Problem sheet

Environment

Please use a Linux environment (e.g., Debian, Ubuntu). A virtual machine is fine. This lab requires a tool called Volatility, which requires Python 2.7.

Provided Materials

- `question-sheet.txt`: A text file for writing your solutions to the tasks.
- `Debian_5.10.0-15-amd64_profile.zip`: A volatility profile for the target computer.
- `dump.elf.gz`: A memory dump of the target computer that has been compromised.

Recommended Tools

- Volatility

Tasks

1. Decompress the memory dump: `gzip -d dump.elf.gz`.
2. Download Volatility: `git clone https://github.com/volatilityfoundation/volatility.git`
3. Add the profile to Volatility:

```
cp Debian_5.10.0-15-amd64_profile.zip \
    volatility/volatility/plugins/overlays/linux/
```

4. Complete and submit `question-sheet.txt`.

Grading

- Question Sheet (See `question-sheet.txt` for grading breakdown)

Hints

- `python ./volatility/vol.py --profile LinuxDebian_5_10_0-15-amd64_profilex64 -f dump.elf --help`
- It is normal to see a lot of import errors when running Volatility. This lab only requires the core modules, which are not dependent on third-party imports.