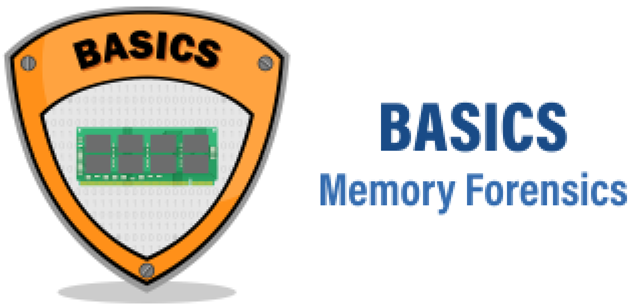

All running processes use memory (RAM or virtual memory) to store code, variables etc. Analysis of memory can be really helpful in recreating the chain of events and recovering important artifacts and information.

In the incident response plan, the incident responders create memory dumps of the live machine to preserve the state of the memory. This memory dump is then processed using various tools to extract information.

What will you learn?

- Analyzing a memory dump using Volatility
- Extracting a binary from a memory dump
- Investigating network connections and programs executed using a memory dump

References:

1. Volatility tool (https://www.volatilityfoundation.org/)

Labs Covered:

- Volatility: Basics
  Analyze the provided memory dump of a Linux machine using the Volatility tool to extract process list, interface details, command history, etc from the memory dump.

- Volatility: Basics II
  Analyze the provided memory dump of a Linux machine and dump the binary from it using the Volatility tool.

- Malware I
  Analyze the provided memory dump of a Linux machine using the Volatility tool to investigate the actions performed during an unauthorized SSH session.

- Volatility: Basic (Windows)
  Analyze the provided memory dump of a Windows machine using the Volatility too to uncover more information like process list, process properties, and open connections, etc.

- Volatility: Basic II (Windows)
  Analyze the provided memory dump of a Windows machine using the Volatility tool to dump a binary, investigate activities of a program, etc.

- Volatility: Binary I
  Analyze the provided memory dump of a Windows machine and investigate a suspicious binary using the Volatility tool.

- Volatility: Binary II
  Analyze the provided memory dump of a Windows machine, dump the password of the logged user using the Volatility tool and decrypt a secret string.

Volatility: Basics

Start

Volatility: Basics II

Start

Malware I

Start

Volatility: Basic (Windows)

Start

Volatility: Binary I

Start

Volatility: Basic II (Windows)

Start

Volatility: Binary II

Start

Privacy Policy ToS