MALAYSIA CYBERSECURITY CAMP

FOXY

ALUMNI 2024

CYBER SKILLS LEVEL-UP! 2023

CYBERSECURITY :

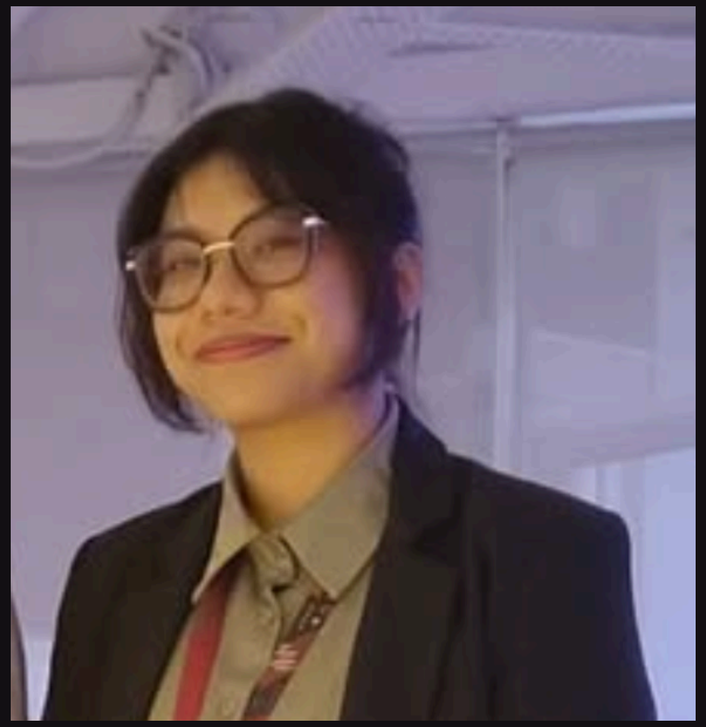
MEMORY ANALYSIS

MALAYSIA CYBERSECURITY CAMP

FOXY

ALUMNI 2024

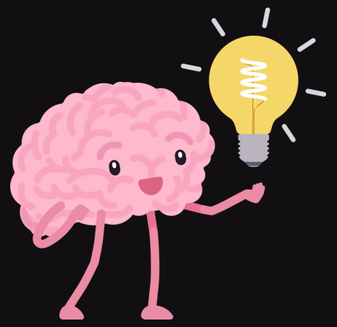
INTRODUCTION



- **ADLINA (FOXY)**
  - Alumni MCC 2024
  - One of the winner for best writeup during MCC 2024
  - Project Manager for BlackBerry CTF 2025 (RE:UN1ON)
  - Seasonal ctf player

MCC
MALAYSIA CYBERSECURITY CAMP

FOXY
ALUMNI 2024



OVERVIEW

Volatile Memory

Memory Dumps

Demo & challenges

MALAYSIA CYBERSECURITY CAMP

FOXY
ALUMNI 2024

OVERVIEW

Volatile Memory

MCC
MALAYSIA CYBERSECURITY CAMP

FOXY
ALUMNI 2024

HOW DO WE DISCOVER THE ATTACKER? BY?

- Disk artifacts
- Logs
- Memory

MCC
MALAYSIA CYBERSECURITY CAMP

FOXY
ALUMNI 2024

HOW DO WE DISCOVER THE ATTACKER? BY?

Memory

MALAYSIA CYBERSECURITY CAMP

FOXY
ALUMNI 2024

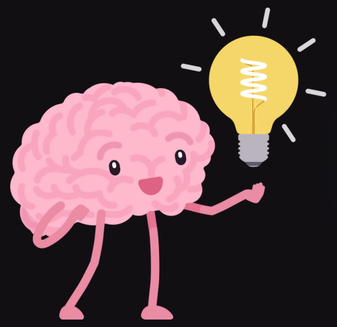
WHY MEMORY?

Memory

- Volatile memory referring to stored data that holds system & user-level data while computers runs.
- System powered off/restarted = data lost
- RAM → temporarily stores everything from open files & running process & encrypted data
- That’s why it is important to investigate as early as possible when investigating RAM.

MCC
MALAYSIA CYBERSECURITY CAMP

FOXY
ALUMNI 2024



MEMORY HIERARCHY

FASTEST

CPU REGISTERS → CPU CACHE → RAM → DISK STORAGE

SLOWEST

MCC
MALAYSIA CYBERSECURITY CAMP

FOXY
ALUMNI 2024

WHAT DOES IT MEAN?

→ CPU registers & cache are extremely fast BUT there's a size limitation

→ RAM is the main working memory for the OS

→ Disk storage is much slower but is very useful for long-term data rentention

MALAYSIA CYBERSECURITY CAMP

FOXY
ALUMNI 2024

IN SHORT:

Disk forensics shows what attackers left behind, memory shows what they're DOING.

MALAYSIA CYBERSECURITY CAMP

FOXY
ALUMNI 2024

OVERVIEW

Memory Dump

MALAYSIA CYBERSECURITY CAMP

FOXY
ALUMNI 2024

MEMORY DUMP?

Memory dump is a snapshot of a system's RAM at a specific point in time.

MCC
MALAYSIA CYBERSECURITY CAMP

FOXY
ALUMNI 2024

HOW IS IT CREATED?

It depends on the operating system in use

kernel mode dumps located at %SystemRoot% \ MEMORY.DMP and hibernation files stored as %SystemDrive% \ hiberfil.sys

Tools like built-in crash dumps, Sysinternals' RAMMap, or third-party utilities such as WinPmem and FTK Imager

MALAYSIA CYBERSECURITY CAMP

FOXY
ALUMNI 2024

TYPES OF MEMORY DUMP

Full Memory Dump

Process Dump

Pagefile and Swap Analysis

MCC
MALAYSIA CYBERSECURITY CAMP

FOXY
ALUMNI 2024

DEMO & CHALLENGE

MALAYSIA CYBERSECURITY CAMP

FOXY

ALUMNI 2024

Q&A SESSION

MALAYSIA CYBERSECURITY CAMP

FOXY
ALUMNI 2024

WRITEUP CHALLENGE:

https://www.notion.so/3ch0/CSLU-GMI-Memory-Analysis-244d05a447d580f9a3bfd93be143e233?source=copy_link

MCC
MALAYSIA CYBERSECURITY CAMP

FOXY
ALUMNI 2024

THANK YOU