



PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE

Applied Computing

Wales Institute of Science and Art (WISA)

Digital Forensics (ACCA7031)

Analysis



[This Photo](#) by Unknown Author is licensed under [CC BY-NC](#)

Lab Activities are based on

TryHackMe, EC Council – CHFI, Digital Forensics Workbook and other Industry Digital Forensic Curriculum

Objectives

In continuation to our lectures, this hands-on Activity helps in providing you an overview of digital forensic analysis.

ETHICAL STATEMENT

As discussed during our lectures, it is very important to adhere to Personal Ethics, Professional Ethics, Computer Ethics and Business Ethics.

We, the participants and stakeholders in the digital forensics laboratory, recognize the significance of ethical conduct when using digital forensics tools and processes for academic purposes. Our commitment to ethical standards is grounded in the principles of integrity, privacy, and responsible handling of digital data.

The tools and techniques you are exposed to' in this lab is to work only on a virtual machine environment and the purpose is entirely to demonstrate various digital forensic activities. Experimentation with these tools, techniques, and resources is at the discretion of the instructor and institution. If you as a student consider using these tools for educational purposes on an outside environment, you should contact your lecturer prior to any experimentation.

Note: Unauthorized access to data, computer, and network systems is a crime in many jurisdictions and often is accompanied by severe consequences, regardless of the perpetrator's motivations. It is the learner's responsibility, as the user of this material, to be cognizant of and compliant with computer use laws.

[illegible]

ICONS Used in this document:

Find out the outcome/ Answers/ Solution



Do research and complete the task. Need referencing/ in-text citations. Shall be included as a part of your coursework.



Recommended Screenshot (with Timestamp) for your Coursework.



Recommended to address this part in your Coursework.

Note: For this activity and other upcoming activities, you shall use any relevant screenshots or discussions to your coursework according to your judgement. I will not be recommending Screenshots/ Recommended part to address in the coursework.

Spectre and Meltdown Vulnerabilities: (Part 1)

A Digital Forensics Investigation (Part 2)

Objective:

To understand the Spectre and Meltdown vulnerabilities, their impact on digital systems, and the forensic analysis implications.

To correlate the vulnerabilities with forensic analysis techniques and incident response.

Requirements:

Part 1

Access to online resources, research papers, and documentation on Spectre and Meltdown.

Virtual machines or test environments for practical analysis.

Part 2

Forensic analysis tools (e.g., Wireshark, volatility, memory dump tools).

Activity Steps: (Part 1)

1. Introduction and Background

Provide an overview of speculative execution, the concepts behind Spectre and Meltdown vulnerabilities, and their impact on modern processors.

Share relevant research papers, articles, and documentation on Spectre and Meltdown for students to review.

2. Literature Review:

Conduct a literature review on Spectre and Meltdown. Understand the technical details of each vulnerability, the affected processor architectures, and potential exploits.

Explore academic papers, security blogs, and official documentation.

3. Practical Analysis

Set up virtual machines or test environments with vulnerable systems.

Simulate or analyze scenarios where Spectre and Meltdown vulnerabilities might be exploited. This could include running proof-of-concept code or examining system behaviors during an attack.

Document the outcome.

4. Correlation with Forensic Analysis (Part 2):

Use forensic analysis tools to capture relevant data, such as memory dumps or network traffic.

Discuss how the information gathered during the practical analysis aligns with typical digital forensics procedures.

Explore:

How might the exploitation of Spectre or Meltdown leave traces in memory or network logs?

What indicators of compromise (IOCs) could be identified during a forensic investigation?

5. Incident Response Scenarios (Part 2):

Pose hypothetical incident response scenarios related to Spectre and Meltdown.

Use the below one or create your own:

An employee with privileged access to the company's financial databases is suspected of exploiting the Spectre vulnerability to retrieve sensitive financial information for personal gain. The incident response team needs to investigate the extent of the compromise and prevent further data leakage.

Analyze memory dumps and system logs to identify any suspicious activities related to Spectre exploitation.

Determine the timeline of the unauthorized access and gather evidence for disciplinary or legal action.

Implement measures to address the vulnerability and prevent similar incidents in the future.

Develop incident response plans, including steps to detect, contain, eradicate, and recover from an incident involving the exploitation of these vulnerabilities.

6. Group Discussion and Reports (Part 3):

Collaborate in groups to discuss their findings, insights, and incident response plans.

Each group should present their analysis and discuss the potential challenges and implications of dealing with Spectre and Meltdown in a real-world digital forensics context.

Reflect on the importance of staying informed about hardware-level vulnerabilities and their impact on forensic investigations.

This activity aims to engage students in both theoretical and practical aspects of digital forensics related to Spectre and Meltdown vulnerabilities, fostering a deeper understanding of the challenges and opportunities in the field.

-----**End of Activity**-----