**INTERNATIONAL QUALIFICATIONS**

**AND ASSESSMENT CENTRE (IQAC)**

«Approved»

________________________

2025 y. «16» cyul

INTERNATIONAL QUALIFICATIONS AND ASSESSMENT CENTRE
XALQARO MALAKALAR VA BAHOLASH MARKAZI
IQAC

| | | | |
|---|---|---|---|
| **Programme** | **LEVEL 5 EXTENDED DIPLOMA IN CYBER SECURITY** | | |
| **Unit Number/ Unit Title** | **UNIT 10 MALWARE ANALYSIS AND REVERSE ENGINEERING** | | |
| **Cohort Code:** | L05MAR-U10 | | |
| **Unit Level** | Level 5 | | |
| **Total GLH** | Total qualification time 200/ Total Guided learning hours 90/ Self-guided learning hours 110 | | |
| **Credits** | 20 CATS/ 10 ECTS | | |
| **Lecturer** | | | |
| **Start Date** | | **End Date** | |

| | |
|---|---|
| **Unit Aims** | To provide students with a thorough understanding of malware, its behaviours, and techniques for analysing and reversing engineered malware. This module focuses on identifying, analysing, and mitigating malware threats. |
| **Differentiation Strategies**<br>*(e.g. planned activities or support for individual learners according to their needs)* | The total number of students to be in the lesson is approximately 20. This is a multicultural group of students predominantly between the ages of 24 – 45, with numerous ethnic, gender, and creed background. These are UK academic level 5 students; hence it is assumed that they have practical, theoretical, or technological knowledge and understanding of a subject or field of work to find ways forward in broadly defined, complex contexts. These students must be able to generate information, evaluate, synthesise the use information from a variety of sources. Various approaches to addressing the various identified students needs will be adopted throughout the lesson. Such will include:-<br>1. Progressive tasks<br>2. Digital resources |

| | |
|---|---|
| | 3. Verbal support<br>4. Variable outcomes<br>5. Collaborative learning<br>6. Ongoing assessment<br>7. Flexible-pace learning |
| **Equality & Diversity** | Variety of teaching techniques will be employed to ensure that the needs of each individual learner are met. |
| **Safeguarding & Prevent** | Safeguarding policies and the Prevent duty are strictly observed to ensure the safety, well-being, and inclusivity of all students and staff. |
| **Health & Safety** | SIRM H&S policies will be maintained. |
| **Learning Resources** | **Teaching and Learning Materials**<br>• "Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software" by Michael Sikorski and Andrew Honig.<br>• "The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory" by Michael Hale Ligh, Andrew Case, Jamie Levy, and Aaron Walters.<br>• "Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation" by Bruce Dang, Alexandre Gazet, and Elias Bachaalany. |

| Learning Outcome | Assessment Criteria |
|---|---|
| **LO1. 1. Understand the fundamentals of malware and its various forms.** | **1. Written Assessments:**<br>1.1 Explain the different types of malwares and their characteristics.<br>1.2 Describe the common propagation methods of malware.<br>1.3 Identify the potential impact of malware on systems and networks. |
| **LO2. 2. Develop skills in static and dynamic malware analysis.** | **2. Practical Assessments:**<br>2.1 Perform static analysis of malware samples using appropriate tools.<br>2.2 Conduct dynamic analysis to observe malware behavior in a controlled environment.<br>2.3 Document and report the findings from malware analysis. |
| **LO3. 3. Apply reverse engineering techniques to deconstruct malware.** | **3. Practical Assessments:**<br>3.1 Use reverse engineering tools and techniques to dissect malware code.<br>3.2 Identify the functionality and purpose of the malware through reverse engineering.<br>3.3 Assess the implications of the malware's behavior on system security. |
| **LO4. 4. Develop strategies for malware detection and mitigation.** | **4. Research and Analysis Assessments:**<br>4.1 Research various methods and tools for malware detection.<br>4.2 Implement techniques to mitigate the effects of malware.<br>4.3 Evaluate the effectiveness of different malware detection and mitigation strategies. |
| **LO5. 5. Understand legal and ethical considerations in malware analysis.** | **5. Written Assessments:**<br>5.1 Discuss the legal implications of malware analysis and reverse engineering.<br>5.2 Explain the ethical considerations involved in handling and analyzing malware.<br>5.3 Describe the responsibilities of a malware analyst in maintaining ethical standards. |

| No | Learning Outcome / Topic | Learning and Teaching Activities | Which assessment criteria does the session relate to? | Day/month/ year/ signature |
|---|---|---|---|---|
| 1 | **Introduction to Malware** | **Introduction to Malware** Definition, history, and evolution of malware. | LO1: Fundamentals of Malware **(Written Assessments)** | |
| 2 | **Types of Malware** | **Types of Malware** Viruses, worms, Trojans, ransomware, spyware, rootkits, botnets, and logic bombs. | LO1: Fundamentals of Malware **(Written Assessments)** | |
| 3 | **Malware Characteristics** | **Malware Characteristics** Payloads, obfuscation techniques, persistence mechanisms. | LO1: Fundamentals of Malware **(Written Assessments)** | |
| 4 | **Propagation Methods** | **Propagation Methods** Phishing, drive-by downloads, exploit kits, USB drops, social engineering. | LO1: Fundamentals of Malware **(Written Assessments)** | |
| 5 | **Impact of Malware** | **Impact of Malware** Data breaches, financial losses, system corruption, network downtime. | LO1: Fundamentals of Malware **(Written Assessments)** | |
| 6 | **Case Studies** | **Case Studies** Analysis of WannaCry, Stuxnet, Zeus, and Emotet. | LO1: Fundamentals of Malware **(Written Assessments)** | |
| 7 | **Static Analysis Fundamentals** | **Static Analysis Fundamentals** File hashing, strings analysis, header inspection. | LO2: Static & Dynamic Malware Analysis **(Practical Assessments)** | |

| | | | | |
|---|---|---|---|---|
| **8** | **Review** | - Review of LO1 topics<br>- Practice questions and mock assessment<br>- **Half-term assessment** based on LO1 (theory) | LO1 LO2 | |
| **9** | **Static Analysis Tools** | **Static Analysis Tools** PEiD, Detect It Easy (DIE), Ghidra, Binwalk. | LO2: Static & Dynamic Malware Analysis **(Practical Assessments)** | |
| **10** | **Dynamic Analysis Setup** | **Dynamic Analysis Setup** Sandbox environments (Cuckoo, Joe Sandbox), VM isolation. | LO2: Static & Dynamic Malware Analysis **(Practical Assessments)** | |
| **11** | **Behavioral Monitoring** | **Behavioral Monitoring** API calls (ProcMon), registry changes, network traffic (Wireshark). | LO2: Static & Dynamic Malware Analysis **(Practical Assessments)** | |
| **12** | **Malware Lab Safety** | **Malware Lab Safety** Best practices for handling live malware samples. | LO2: Static & Dynamic Malware Analysis **(Practical Assessments)** | |
| **13** | **Reporting Findings** | **Reporting Findings** Documenting IOCs (Indicators of Compromise) and TTPs (Tactics, Techniques, Procedures). | LO2: Static & Dynamic Malware Analysis **(Practical Assessments)** | |
| **14** | Review | - Comprehensive review of all learning outcomes<br>- Practice questions and revision of key topics | | |
| **15** | Midterm | - **Midterm assessment** covering all learning outcomes (theory and practical elements) | | |

| | | | | |
|---|---|---|---|---|
| **16** | Feedback & Reflection | - Review<br>- Individual feedback on performance<br>- Reflective discussion on key learning points | | |
| **17** | **Reverse Engineering Basics** | **Reverse Engineering Basics** Disassembly vs. decompilation, x86/x64 architecture. | LO3: Reverse Engineering Malware **(Practical Assessments)** | |
| **18** | **Tools for Reverse Engineering**. | **Tools for Reverse Engineering** IDA Pro, Ghidra, x64dbg, OllyDbg. | LO3: Reverse Engineering Malware **(Practical Assessments)** | |
| **19** | **Analyzing Malicious Code** | **Analyzing Malicious Code** Identifying functions, loops, and malicious logic. | LO3: Reverse Engineering Malware **(Practical Assessments)** | |
| **20** | **Debugging Techniques** | **Debugging Techniques** Breakpoints, memory dumping, stepping through code. | LO3: Reverse Engineering Malware **(Practical Assessments)** | |
| **21** | **Unpacking Malware** | **Unpacking Malware** Detecting UPX, Themida, and other packers. | LO3: Reverse Engineering Malware **(Practical Assessments)** | |
| **22** | **Extracting Threat Intelligence** | **Extracting Threat Intelligence** C2 (Command & Control) server analysis, payload extraction. | LO3: Reverse Engineering Malware **(Practical Assessments)** | |
| **23** | **Review** | **Detection Methods** Signature-based, heuristic, behavioral, and AI-driven detection. | LO4: Malware Detection & Mitigation **(Research & Analysis Assessments)** | |
| **24** | **Detection Tools** | **Detection Tools** YARA rules, Snort, Suricata, EDR solutions (CrowdStrike, SentinelOne). | LO4: Malware Detection & Mitigation **(Research & Analysis Assessments)** | |

| | | | | |
|---|---|---|---|---|
| **25** | **Mitigation Strategies** | **Mitigation Strategies** Patch management, least privilege, network segmentation. | LO4: Malware Detection & Mitigation **(Research & Analysis Assessments)** | |
| **26** | **Incident Response** | **Incident Response** Containment, eradication, recovery, and post-mortem analysis. | LO4: Malware Detection & Mitigation **(Research & Analysis Assessments)** | |
| **27** | **Legal Frameworks** | **Legal Frameworks** CFAA, GDPR, DMCA, and responsible disclosure laws. | LO5: Legal & Ethical Considerations **(Written Assessments)** | |
| **28** | **Ethics in Malware Analysis** | **Ethics in Malware Analysis** Safe handling, privacy protection, and professional responsibilities | LO5: Legal & Ethical Considerations **(Written Assessments)** | |
| **29** | Final Exam Preparation & Review | LO1, LO2, LO3, LO4 | LO1, LO2, LO3, LO4 | |
| **30** | Final Exam | | LO1, LO2, LO3, LO4 | |