Unit Outline (Higher Education)

Institute / School: Global Professional School

Unit Title: CYBERSECURITY: MALWARE ANALYSIS

Unit ID: GPSIT1011

Credit Points: 15.00

Prerequisite(s): Nil

Co-requisite(s): Nil

Exclusion(s): Nil

ASCED: 029901

Description of the Unit:
This project aims to prepare Engineering students and other aspiring cybersecurity professionals on malware analysis and detection. Working within the environment of a cybersecurity department, the teams will perform static and dynamic analysis of an identified malware and will gain an understanding of the process for the reverse engineering of malware. Experience of these processes will help learners gain skills in the most critical challenge faced by organisations in the fast-evolving digital era. The team will produce reports on their work and make their colleagues aware of potential vulnerabilities.

Grade Scheme: Ungraded (S, UN)

Work Experience:

No work experience: Student is not undertaking work experience in industry.

Placement Component: No

Supplementary Assessment: No

Supplementary assessment is not available to students who gain a fail in this Unit.

Course Level:

Level of Unit in Course	AQF Level of Course					
	5	6	7	8	9	10
Introductory			✔			
Intermediate						
Advanced						

Learning Outcomes:

Knowledge:

K1. Understand the reason for system malfunction
K2. Understand impacts of Malware
K3. Understand how to analyse the network behaviour of unknown malwares
K4. Understand how to set up a baseline analysis environment and determine a starting point for triaging

Skills:

S1. Use hash value to research the details of malware
S2. Use tools to explore DLLs and functions imported by malware
S3. Use utilities to help manage, troubleshoot and diagnose Windows systems and applications
S4. Work effectively in a team

Application of knowledge and skills:

A1. Perform static analysis of malware
A2. Perform dynamic analysis of malware
A3. Simulate Malware to identify the impact on network
A4. Create a response plan to detect and protect - plan and execute reverse engineering

Unit Content:

Teams will perform static and dynamic analysis of an identified malware and will gain an understanding of the process for the reverse engineering of malware.

Topics may include:

- Sprint 1 (2 Weeks)
  Gain a complete understanding of the problem scenario. Complete installation of requisite tools/software needed for static and dynamic analysis. Prepare the required lab environment needed for analysis and debugging.
- Sprint 2 (2 Weeks)
  Define a project plan, standard operating procedures and reporting templates to document all findings, roles and responsibilities and recommendations.
- Sprint 3 (2 Weeks)
  Confirm details affecting system changes on endpoints. Understand how processes executed by machine effect system behavioural change.
- Sprint 4 (2 Weeks)
  Course Outline (Higher Education) Identify existing processes running on a system and learn how to sniff the packets through the machine. Implement software suite for simulating common internet services in a lab environment.
- Sprint 5 (2 Weeks)
  Undertake complete static and dynamic analysis flow for malware by setting up a baseline analysis environment and triaging to determine a starting point.
  Perform static analysis to get a sense of where everything is before debugging.
  Perform dynamic analysis to determine behaviours that cannot be understood by static analysis.
- Sprint 6 (2 Weeks)
  Perform manual debugging by stepping through the program to navigate until the malware is identified.
  Perform reverse engineering to find hard-coded passwords and create a response plan.

FEDTASKS

Federation University Federation recognises that students require key transferable employability skills to prepare them for their future workplace and society. FEDTASKS (**T**ransferable **A**ttributes **S**kills and **K**nowledge) provide a targeted focus on five key transferable Attributes, Skills, and Knowledge that are be embedded within curriculum, developed gradually towards successful measures and interlinked with cross-discipline and Co-operative Learning opportunities. *One or more FEDTASK, transferable Attributes, Skills or Knowledge must be evident in the specified learning outcomes and assessment for each FedUni Unit, and all must be directly assessed in each Course.*

FEDTASK attribute and descriptor		**Development and acquisition of FEDTASKS in the Unit**	
		Learning Outcomes (KSA)	**Assessment task (AT#)**
FEDTASK 1 Interpersonal	Students will demonstrate the ability to effectively communicate, inter-act and work with others both individually and in groups. Students will be required to display skills in-person and/or online in: • Using effective verbal and non-verbal communication • Listening for meaning and influencing via active listening • Showing empathy for others • Negotiating and demonstrating conflict resolution skills • Working respectfully in cross-cultural and diverse teams.	K1, S1-2, S4 A1, A2	AT1
FEDTASK 2 Leadership	Students will demonstrate the ability to apply professional skills and behaviours in leading others. Students will be required to display skills in: • Creating a collegial environment • Showing self -awareness and the ability to self-reflect • Inspiring and convincing others • Making informed decisions • Displaying initiative	K2-4, S1-4, A3-4	AT1-AT2
FEDTASK 3 Critical Thinking and Creativity	Students will demonstrate an ability to work in complexity and ambiguity using the imagination to create new ideas. Students will be required to display skills in: • Reflecting critically • Evaluating ideas, concepts and information • Considering alternative perspectives to refine ideas • Challenging conventional thinking to clarify concepts • Forming creative solutions in problem solving.	K1-3, S1-3, A1-4	AT2-AT3 AT5-AT6

FEDTASK attribute and descriptor		Development and acquisition of FEDTASKS in the Unit	
		Learning Outcomes (KSA)	**Assessment task (AT#)**
FEDTASK 4 Digital Literacy	Students will demonstrate the ability to work fluently across a range of tools, platforms and applications to achieve a range of tasks. Students will be required to display skills in: • Finding, evaluating, managing, curating, organising and sharing digital information • Collating, managing, accessing and using digital data securely • Receiving and responding to messages in a range of digital media • Contributing actively to digital teams and working groups • Participating in and benefiting from digital learning opportunities.	K1, K3-4, S2-3, S4 A 3-4	AT3, AT5, AT6
FEDTASK 5 Sustainable and Ethical Mindset	Students will demonstrate the ability to consider and assess the consequences and impact of ideas and actions in enacting ethical and sustainable decisions. Students will be required to display skills in: • Making informed judgments that consider the impact of devising solutions in global economic environmental and societal contexts • Committing to social responsibility as a professional and a citizen • Evaluating ethical, socially responsible and/or sustainable challenges and generating and articulating responses • Embracing lifelong, life-wide and life-deep learning to be open to diverse others • Implementing required actions to foster sustainability in their professional and personal life.	K1-2, S3-4, A4	AT2, AT3, AT4, AT5, AT6

Learning Task and Assessment:

Learning Outcomes Assessed	Assessment Tasks	Assessment Type	Weighting
K1-2 S1-2, S4 A1	Documenting findings about the type of malware file, compiler used, the encrypting tool, the packer and protector used. Documenting findings about when the executable was compiled, the timeframe of attack and corresponding deductions.	Team report and presentation	S/U
K1-2 S1-2, S4 A1	Documenting findings about information gathered on malicious DLLs, processes using those DLLs (if any), determining whether DLL is loaded into a process after load time, comparison of DLL list in Process Explorer vs imports shown in Dependency Walker.	Team report and presentation	S/U
K2-4 S2-4 A2	Documenting findings about impact on system and process	Team report and presentation	S/U

Learning Outcomes Assessed	Assessment Tasks	Assessment Type	Weighting
K2-4 S2-4 A2	Documenting findings on performance impact Documenting findings on network impact	Team report and presentation	S/U
K3-4 S2-4 A1-4	Documenting the steps followed and observations during: 1. Completing the process of static analysis 2. Completing the process of dynamic analysis	Team report and presentation	S/U
K3-4 S2-4 A1-4	Documenting the steps followed and observations during: 1. Completing the process of anti-debugging 2. Documenting the recommendations to protect the system from malware	Team report and presentation	S/U

Adopted Reference Style:

APA

Refer to the library website for more information

Fed Cite - referencing tool