WM179-18 Cyber Fundamentals

22/23

Department
WMG
Level
Undergraduate Level 1
Module leader
Harjinder Lallie
Credit value
18
Module duration
30 weeks
Assessment
Multiple
Study location
University of Warwick main campus, Coventry

Description

Introductory description

Understanding the steps and common attack patterns associated with cyber is essential to detecting, identifying, mitigating and responding to cyber-attacks.

Working on this module you will develop knowledge of these core concepts. You will also gain insight into how adversaries move from initially probing and performing reconnaissance of targets, to implementing a way to persist and maintain access to a device/network once compromised.

Several frameworks and attack modelling techniques exist to help better understand and conceptualize how adversaries move through the stages of a cyber-attack have come to the forefront of the cyber security industry. These include: attack graphs, attack trees, fault trees, MITRE ATT&CK, Cyber Kill Chain. Some of these techniques enable practitioners to model a cyber-attack using visual methods.

This module equips students to better understand the stages and concepts of a cyber-attack. Additionally, the module will equip and allow students to develop a practical understanding, as well as applying a range of tools, techniques and procedures utilized by adversaries and attackers during each phase of a cyber-attack in a manner that is both legal and ethical.

Module aims

The module aims to enable students to:

- understand and apply common cyber-attack modelling methods.
- apply the common tools, techniques and procedures associated with cyber-attacks, legally, ethically, and methodically.

Outline syllabus

This is an indicative module outline only to give an indication of the sort of topics that may be covered. Actual sessions held may differ.

Cyber Landscape
Linux Command Line, Bash Scripting, and automation
Common cyber-attack modelling systems including: attack graphs, attack trees, fault trees, MITRE ATT&CK, Cyber Kill Chain
Vulnerability testing in a corporate context
Legal and Ethical considerations
Active and passive reconnaissance
Re-purposing
Delivery
Exploitation
Installation
Command & Control(C2)
Action on objectives

Learning outcomes

By the end of the module, students should be able to:

- Using a given framework, identify tools, techniques and procedures which are associated with common attacks within the context of cyber-space
- Compare and contrast the effectiveness of the relevant tools, techniques and procedures of a given cyber-attack framework when employed against a given target system.
- Demonstrate the application of the tools, techniques and procedures of a given cyber-attack framework which may be used by cyber adversaries against a simulated target system.
- Demonstrate the ability to communicate complex cyber-attack primitives to lay audiences concisely, clearly, and professionally

Indicative reading list

- Yadav, T., & Rao, A.M. (2015). Technical Aspects of Cyber Kill Chain. SSCC.
- Cooper, M.(2014). Advanced Bash Scripting Guide.

Subject specific skills

- Select and apply appropriate tools, techniques and procedures related to specific parts of the Cyber Kill Chain.
- Identify tools, techniques and procedures that could be used to mitigate and remediate the actions of an adversary.

- Respond appropriately to situations that challenge legal, ethical and reputational values.

Transferable skills

Problem solving, critical thinking, creativity, analytical and ethical reasoning

---

Study

Study time

Type	Required
Supervised practical classes	18 sessions of 3 hours (28%)
Private study	42 hours (21%)
Assessment	100 hours (51%)
Total	196 hours

Private study description

Independent activity between workshops.

Costs

No further costs have been identified for this module.

Assessment

You do not need to pass all assessment components to pass the module.

Assessment group A

	Weighting	Study time
Coursework 1	50%	50 hours
Analysis, evaluation, and modelling of a recent cyber-attack represented within a report aimed at given stakeholders		
Coursework 2	50%	50 hours
Application and analysis of vulnerability testing strategies to a synthetic target.		

Assessment group R

	Weighting	Study time
Coursework	100%	

Application and analysis of vulnerability testing strategies to a synthetic target.

Feedback on assessment

Via Tabula

Availability

Courses

This module is Core for:

- UWMA-H651 Undergraduate Cyber Security
  - Year 1 of H651 Cyber Security
  - Year 1 of H651 Cyber Security
  - Year 1 of H651 Cyber Security