# WM179-18 Cyber Fundamentals

## 24/25

**Department**
WMG
**Level**
Undergraduate Level 1
**Module leader**
Harjinder Lallie
**Credit value**
18
**Module duration**
30 weeks
**Assessment**
100% coursework
**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.

To better understand these concepts learners are introduced to basic organisational/cultural concepts around managing cyber security, protecting organisations from harm, and developing fundamental cyber security policy and procedures to enable such protection.

## 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.

*The Cyber Landscape in an organisational and national/international context*

- Managing cyber security
- Protecting organisations from harm
- Developing cyber security policy and procedures to enable such protection
- Cyber security culture
- Secure cyber infrastructures

*Attack Modelling*
Common cyber-attack modelling systems including: attack graphs, attack trees, fault trees, MITRE ATT&CK, Cyber Kill Chain

Linux Command Line, Bash Scripting, and automation

*Vulnerability testing*

- Legal and Ethical considerations
- Active and passive reconnaissance
- Re-purposing
- Delivery
- Exploitation
- Installation
- Command & Control(C2)
- Action on objectives
- Writing vulnerability testing reports

## 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 [CITP, 2.1.1][AHEP, C7, C8, C10, C11]
- 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. [CITP, 2.1.2,

2.1.4, 2.1.9, 2.2.2][AHEP, C7, C8, C10]
- 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. [CITP, 2.1.5, 2.1.7, 2.1.8, 2.3.1][AHEP, C7, C8 ]
- Demonstrate the ability to communicate complex cyber-attack primitives to lay audiences concisely, clearly, and professionally. [CITP, 2.1.2][AHEP, C7, C8]

## Indicative reading list

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

View reading list on Talis Aspire

## 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 |
|---|---|
| Lectures | 18 sessions of 1 hour (10%) |
| Supervised practical classes | 36 sessions of 1 hour (20%) |
| Private study | 66 hours (37%) |
| Assessment | 60 hours (33%) |
| Total | 180 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 A1

| | Weighting | Study time | Eligible for self-certification |
|---|---|---|---|
| **Assessment component** | | | |
| Coursework 1 | 50% | 48 hours | Yes (extension) |
| Analysis, evaluation, and modelling of a recent cyber-attack represented within a report aimed at given stakeholders | | | |
| **Reassessment component is the same** | | | |
| **Assessment component** | | | |
| Practical test | 50% | 12 hours | No |
| Practical test testing the ability to perform a vulnerability test against a specified target or targets | | | |
| **Reassessment component is the same** | | | |

### Feedback on assessment

Via Tabula

---

## Availability

## Courses

This module is Core for:

- Year 1 of UWMA-H651 Undergraduate Cyber Security