WM9C2-15 Proactive Cyber Defence

24/25

Department
WMG
Level
Taught Postgraduate Level
Module leader
Christo Panchev
Credit value
15
Module duration
4 weeks
Assessment
100% coursework
Study location
University of Warwick main campus, Coventry

Description

Introductory description

This module seeks to introduce the students to the state-of-the-art in effective and proactive cyber defensive methodologies and strategies, including tools and techniques that can have long-term benefits in organisational policies while maintaining the resilience of our agile and delicate cyber infrastructures.

Module aims

This module aims to introduce the students in the fundamental security operations strategies and emerging tools, techniques and approaches to deter advanced cyber attacks and mitigate their impact, including cyber infrastructure security monitoring, detection and incident response.

The module equips the participants with an in-depth understanding of the fail-safe capabilities of different systems and mechanisms used to analyse targeted and multi-stage cyber attacks. Students will establish a firm and in-depth knowledge in network security protocols, including their design philosophy and their weaknesses exploited by motivated and resourceful adversaries.

The module also seeks to equip students with the technical explication of threat modelling in identifying and ranking threats against a variety of scenarios using industry-led and experimental approaches. Students are expected to critically synthesise tools and approaches to adequately model threat landscapes against efficient and autonomous information systems while transferring

these skills in different areas where potential threats to business operations might be present.

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.

- Vulnerabilities. Constituent elements of a vulnerability: pre-conditions, pre-condition logic, exploits, post-conditions. Vulnerability inventories, disclosure and mitigation; Standard Security Description references; Cyber mission system development frameworks; Cyber defence measurables & evaluation criteria. Vulnerability and Attack surface management.
- Intelligence gathering for adaptive network defence; Kill-chain model, MITRE and the APTs paradigm; STIX and CybOX; Threat actors. Cyber criminals, hacktivists, state-sponsored attackers (advanced persistent threats) and insider threats (malicious, incompetence, negligence); Cyber threat analytics
- Semantic network and threat modelling techniques. Attack graphs, attack trees and fault trees. The application of attack modelling techniques in aiding attack analysis, event prediction, outlining of mitigation strategies. investigation of incidents and system hardening; STRIDE; DREAD; Experimental approaches; Threat Model Validation & DFDs; Diagram types & Trust Boundaries
- Security Operations. SOC structure and processes. Security monitoring, detection and response. Incident Response.Threat hunting.

Learning outcomes

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

- Critically synthesise and apply knowledge and skills in detecting, denying, disrupting, and destroying capabilities of adversarial actors.
- Demonstrate an in-depth and systematic understanding of methodologies, tools and techniques used in network defence and attack analysis in terms of their effectiveness and suitability in different organisational contexts and threat landscapes.
- Analyse cyber threats and potential cyber attacks using established modelling techniques and frameworks, and use the findings to inform the deployment of defensive cyber security operations.
- Flexibly and autonomously apply knowledge on the creation of innovative and pragmatic solutions in network defence as a response to multi-faced, sophisticated and destructive cyber attacks

Indicative reading list

Anderson, Ross J., “Security Engineering: A Guide to Building Dependable Distributed Systems”, 2 Ed, John Wiley & Sons (2008)
Nathans, David, “Designing and Building a Security Operations Center”, Syngress (2014)
Caravelli, J. and Jones, N., 2019. Cyber Security: Threats and Responses for Government and Business. ABC-CLIO.
Wang, C. and Lu, Z. eds., 2019. Proactive and Dynamic Network Defense. Springer International

Publishing.
Svensson, Robert, “From Hacking to Report Writing: An Introduction to Security and Penetration Testing”, Apress (2016)

View reading list on Talis Aspire

Research element

There is a strong emphasis on the development, growth and enhancement of individual research skills so as to provide participants with the high level research knowledge, skills and competencies needed to undertake an independent, original piece of research. The module content draws upon and highlights research within the domain and the module assessment requires participants to perform further research before preparing a response to the assessment task.

Subject specific skills

Participants will develop an advanced understanding and technical skills in a number of network and computer security principles, strategies, techniques and concepts in cyber security operations

Transferable skills

Critical and analytical thinking, problem solving, communication, professionalism, organise and manage critical resources such as time, budget and finance

---

Study

Study time

Type	Required
Supervised practical classes	30 sessions of 1 hour (20%)
Private study	60 hours (40%)
Assessment	60 hours (40%)
Total	150 hours

Private study description

Further practical lab work and research.

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 A2

	Weighting	Study time	Eligible for self-certification
Case Study on Threat Identification and System Hardening	100%	60 hours	Yes (extension)

The work will involve the use of tools, methods and techniques for network hardening, attack analysis and projection in a given case study related to security breaches and incidents. This work will enable students to actively reflect upon the given case, critically analyse the techniques used, evaluate threats, benefits and limitations and propose alternative (optimal) solutions. Students will be asked to demonstrate certain solutions as part of their hands-on work and evidence of protection against network-based attacks in a given case using appropriate forms of reporting.

Feedback on assessment

Feedback will be provided on a standard WMG feedback form.

Availability

There is currently no information about the courses for which this module is core or optional.