ES94P-15 Security Architectures and Network Defence

22/23

Department
WMG
Level
Taught Postgraduate Level
Module leader
Peter Norris
Credit value
15
Module duration
1 week
Assessment
Multiple
Study location
University of Warwick main campus, Coventry

Description

Introductory description

It is assumed that students will already have some background in conventional, potentially insecure, data networks that is patchy and worthy of review. In particular, IPv4, and TCP / UDP are thoroughly covered, supported by extensive analysis of traffic flows using visualisation tools such as wireshark.

Security architectures to segregate differing trust domains via security devices, especially stateful packet filtering firewalls, are introduced and analysed, together with the mindset that any particular defence will fail at some point, necessitating layered defence in depth.

Module aims

To equip students to use tools and techniques to improve the security of an organisation's network.

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 security landscape:
terminology (CIA, AAA, asset, threat, vulnerability, exploit, mitigation)
threats (malware, phishing, pharming, social engineering, insider)
attack surfaces (people, processes, technology, physical).

Network defence:
IP4 networks, addressing, routing, network architecture, trust domains,
TCP/UDP, packet capture and analysis using wireshark,
experimentation with virtual networks, dual-use tools (nmap, ettercap)
ingress and egress filtering via (stateful) packet firewalls
patterns of attack and related intervention, detection and prevention techniques,
network security testing, concepts, tools, issues,
network security monitoring, passive, proactive, technical, non-technical, consequences
network security audit.

Learning outcomes

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

- Critically evaluate the security posture of a network
- Recommend security configuration adjustments to achieve a desired security posture
- Apply security configuration adjustments to achieve a desired security posture
- Verify the extent to which configuration adjustments achieve the intended security posture.

Indicative reading list

IETF, “IETF Request for Comments (RFC)”, https://www.ietf.org/rfc/ [accessed 26 May 2020]

Pfleeger, C. P. and Pfleeger S. L. , "Security in Computing", 4 ed. vol. 604: Prentice Hall, 2007.

Anderson R. , "Security Engineering: A guide to building dependable distributed systems", 2 ed.: Wiley, 2008.

Donahue, Gary A., “Network Warrior”, O'Reilly (2011)

Kozeriok, Charles M., “TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference”, No Starch Press (2005)

Subject specific skills

Manipulate network security.

Transferable skills

Problem solving, digital literacy, organisatonal awareness

Study

Study time

Type	Required
Lectures	10 sessions of 1 hour (7%)
Tutorials	10 sessions of 1 hour (7%)
Practical classes	10 sessions of 1 hour (7%)
Online learning (scheduled sessions)	(0%)
Online learning (independent)	60 sessions of 1 hour (40%)
Assessment	60 hours (40%)
Total	150 hours

Private study description

No private study requirements defined for this module.

Costs

No further costs have been identified for this module.

Assessment

You must pass all assessment components to pass the module.

Assessment group A1

	Weighting	Study time	Eligible for self-certification
Coursework	100%	60 hours	Yes (extension)

A single assessment component which requires the implementation of a network design exercise. The design must be provably secure.

Assessment group R

	Weighting	Study time	Eligible for self-certification
Assessed work as specified by department	100%		Yes (extension)

100% Assignment

Feedback on assessment

Written feedback provided with the mark via tabula.

Availability

Anti-requisite modules

If you take this module, you cannot also take:

- ES94P-10 Security Architectures and Network Defence

Courses

This module is Core optional for:

- Year 1 of TWMA-H6C7 Postgraduate Taught Cyber Security Engineering