Practical Sysadmin Security

Module Information

2022.01, Approved

Summary Information

Module Code	7137COMP
Formal Module Title	Practical Sysadmin Security
Owning School	Computer Science and Mathematics
Career	Postgraduate Taught
Credits	20
Academic level	FHEQ Level 7
Grading Schema	50

Teaching Responsibility

LJMU Schools involved in Delivery
Computer Science and Mathematics

Learning Methods

Learning Method Type	Hours
Lecture	12
Practical	24

Module Offering(s)

Display Name	Location	Start Month	Duration Number Duration Unit
JAN-CTY	CTY	January	12 Weeks

Aims and Outcomes

Aims	To allow students to develop new advanced security skills and to combine their existing and new skills in a practical context. Students will use real-world Cloud-based and locally administered systems to apply their knowledge to.

After completing the module the student should be able to:

Learning Outcomes

Code	Number	Description
MLO1	1	Understand the relationship between theoretical and practical security concepts and implementation.
MLO2	2	Apply security concepts to the hardening of existing systems and networks.
MLO3	3	Use pen-testing, configuration and rapid-response techniques to prevent and respond to security breaches.
MLO4	4	Use investigatory skills to perform post-mortem analysis of security breaches.
MLO5	5	Appreciate the challenges involved in managing security in an enterprise environment.

Module Content

Outline Syllabus	Practical cryptography (PGP/GnuPG, keychains, trust, creating certificates)Using the secure shell (SSH, SCP, port forwarding)Web server security (Web Server configuration, TLS/SSL configuration, proxies and caches, DMZ, web log analysis, encrypted database records and salting)Firewalls and intrusion detection systemsCloud security (Cloud system security configuration, virtual machines, security profiles, compliance)Privacy (onion routing and Tor, Web tracking, system logs, full disk encryption)Access control and authentication (LDAP, Kerberos, Active Directory, SELinux)Enterprise security (policy, provisioning, BYOD, multiuser systems, application security, secure networking)Application security (interpreters and macros, data encryption, software installation)Mobile security (sandboxing, permissions, app-store policies)Mitigation (backup strategies, console scripting)Patches and vulnerabilities (CVE, CERTs, patch management, incident response)Post-mortem investigation (logfile analysis, attack tree analysis)
Module Overview	The module provides an opportunity to learn and practice systems administration skills for security. You will develop advanced security skills and apply them in a practical context. You will use real-world Cloud-based and locally administered systems to apply your knowledge.
Additional Information	The module provides an opportunity to learn and practice systems administration skills for security.

Assessments

Assignment Category	Assessment Name	Weight	Exam/Test Length (hours)	Module Learning Outcome Mapping
Report	Hardened system implementation	50	0	MLO2, MLO3
Report	Secure system design	50	0	MLO1, MLO4, MLO5

Module Contacts

Module Leader

Contact Name	Applies to all offerings	Offerings
Nathan Shone	Yes	N/A

Partner Module Team

Contact Name	Applies to all offerings	Offerings