Liverpool John Moores University

Warning: An incomplete or missing proforma may have resulted from system verification processing

Title:	PRACTICAL SYSADMIN SECURITY
Status:	Definitive
Code:	**7052COMP** (120627)
Version Start Date:	01-08-2019
Owning School/Faculty:	Computer Science
Teaching School/Faculty:	Computer Science

Team	Leader
Nathan Shone	Y

Academic Level:	FHEQ7	**Credit Value:**	20	**Total Delivered Hours:**	36
Total Learning Hours:	200	**Private Study:**	164		

Delivery Options
Course typically offered: Semester 2

Component	**Contact Hours**
Lecture	12
Practical	24

Grading Basis: 40 %

Assessment Details

Category	**Short Description**	**Description**	**Weighting (%)**	**Exam Duration**
Artefacts	AS1	Implementation of a hardened system based on a given specification	50	
Report	AS2	Report covering secure system design	50	

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.

Learning Outcomes

After completing the module the student should be able to:

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

Learning Outcomes of Assessments

The assessment item list is assessed via the learning outcomes listed:

Hardened system implementation	2	3	
Secure system design	1	4	5

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 systems
Cloud 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)

Learning Activities

The module will provide both theoretical and practical elements. The theoretical work will largely build on existing theoretical knowledge, recapping and refocussing on its application to real systems. The practical element will involve hands-on system configuration and security response. Assessment will include a practial element that will also contribute as a learning activity.

Notes

The module provides an opportunity to learn and practice systems administration skills for security.