MACS H6019: Application Security

Short Title:	Application Security APPROVED
Full Title:	Application Security

Module Code:	MACS H6019

ECTS credits:	10

NFQ Level:	9

Module Delivered in	2 programme(s)

Module Contributor:	Anthony Keane

Module Description:	This module covers the weakness of applications (web and system) to attack from Internet and other sources. Best practice safety policies and procedures are covered as well as how to test and measure the vulnerabilities of systems.

Learning Outcomes:

On successful completion of this module the learner will be able to

1. Evaluate, appraise and classify the threats to a computer system based on host applications
2. Measure and reduce the vulnerability of computer system applications
3. Communicate threat analysis outputs to decision makers using reports and presentations

Module Content & Assessment

Indicative Content
Overview Introduction to Application Security, Cyber Threats, Need for securing systems and applications, Types of security vulnerabilities
Reconnaissance and Mapping Mapping the infrastructure. Identify the machines, operating systems and applications. configurations and weaknesses. Explore virtual hosting and its impact on security. Explore external information sources. Google hacking. Using tools. Scripting to automate processes. Application flow charting. Relationship analysis within an application.
Client Side Discovery Learn methods to discover various vulnerabilities. Information leakage. Username harvesting. Command injection. SQL injection. Blind SQL injection. Cross-Site Scripting (XSS). Cross-Site Request Forgery. Methods to decompile client-side code. Explore malicious applets and objects. Discovery vulnerabilities in Web application through their client components.Understand methods for attacking Web services. Understand methods for testing sites. The ability to extend the tools we are using.
Server Side Discovery Learn methods to discover various vulnerabilities. Information leakage. Username harvesting. Command injection. SQL injection. Blind SQL injection. Cross-Site Scripting (XSS). Cross-Site Request Forgery. Session issues. Explore differences between different data back-ends. Explore fuzzing and various fuzzing tools. Understand methods for attacking Web services
Exploiting internal networks. Explore attack frameworks. AttackAPI. BeEF. XSS-Proxy Walk through an entire attack scenario. Exploit the various vulnerabilities discovered. Leverage the attacks to gain access to the system. Learn how to pivot our attacks through a Web application. Understand methods of interacting with a server through SQL injection. Exploit applications to steal cookies. Execute commands through Web application vulnerabilities

Indicative Assessment Breakdown	%
Course Work Assessment %	100.00%

Course Work Assessment %

Assessment Type	*Assessment Description*	*Outcome addressed*	*% of total*	*Assessment Date*
Practical/Skills Evaluation	Build and test a computer network of typical applications used by companies and organizations.	2	50.00	Week 11
Written Report	Investigative report on threats and vulnerabilities to applications.	1	30.00	Week 6
Presentation	Presentation of the mini-project conducted by the student throughout the course.	3	20.00	Week 11

No Final Exam Assessment %

Indicative Reassessment Requirement
Coursework Only *This module is reassessed solely on the basis of re-submitted coursework. There is no repeat written examination.*

ITB reserves the right to alter the nature and timings of assessment

Indicative Module Workload & Resources

Indicative Workload: Full Time	
Frequency	**Indicative Average Weekly Learner Workload**
Every Week	30.00
Every Week	30.00
Every Week	140.00

Resources

Recommended Book Resources

Bryan Sullivan, Vincent Liu, *Web Application Security, A Beginner's Guide*, McGraw-Hill Osborne Media [ISBN: 0071776168]

Dafydd Stuttard, Marcus Pinto, *The Web Application Hacker's Handbook*, Wiley [ISBN: 1118026470]

Michal Zalewski, *The Tangled Web*, No Starch Press [ISBN: 1593273886]

Jon Erickson, *Hacking: The Art of Exploitation, 2nd Edition*, No Starch Press [ISBN: 1593271441]

This module does not have any article/paper resources

Other Resources

Website: *Open Web Application Security Project (OWASP)*
https://www.owasp.org/

Website: *Web Application Security Consortium*
http://www.webappsec.org/

Website: *Security Development Lifecycle*
https://www.microsoft.com/en-us/SDL/Defa ult.aspx

Module Delivered in

Programme Code	Programme	Semester	Delivery
BN_KMACS_R	Master of Science in Computing in Applied Cyber Security	2	Elective
BN_KMACS_M	Master of Science in Computing in Applied Cyber Security (Research)	1	Group Elective 2