H9IRSAN: Incident Response and Analytics

Module Code:	H9IRSAN
Long Title	Incident Response and Analytics CONDITIONAL APPROVAL
Title	Incident Response and Analysis
Module Level:	LEVEL 9
EQF Level:	7
EHEA Level:	Second Cycle

Credits:	5

Module Coordinator:	Simon Caton

Module Author:	Margarete Silva

Departments:	School of Computing

Specifications of the qualifications and experience required of staff	

Learning Outcomes

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

#	Learning Outcome Description
LO1	Compare, contrast and apply appropriate incident response principles and methodologies.
LO2	Assess and evaluate IT systems and networks for compromise.
LO3	Perform proficiently in incident management from an initial compromise to recovery and make recommendations on how to improve the infrastructure to enhance both security and detection.

Dependencies

Module Recommendations

No recommendations listed

Co-requisite Modules

No Co-requisite modules listed

Entry requirements	

H9IRSAN: Incident Response and Analytics

Module Content & Assessment

Indicative Content

Network Security Design Principles and Fundamentals
• Defence-in-Depth concepts o Firewalls, Proxies, Load-Balancers etc. • System Security concepts o High-level introduction to Windows and Linux OS Security

Cyber Attack Incident Response Preparation, Methodologies & Principles
• Incident Response Steps • Assessing Impact of Cyber Attacks • Scaling Incident Response • Threat Intelligence • OpSec

Logging, Monitoring & Forensics
• Why Log? • Where to log and how o Types of Logs o Where Logging should be done o Challenges of logging with compliance • System Forensics and tools – Windows and Linux Operating Systems: o Automated Collection o Malware Standard Response Pattern o Volatile Data Investigation o Other Windows Artifact Investigation o Other Linux Artifact Investigation • Introduction to the types of network data • How to collect & store data for Incident Response • Incidences based around applications and people

Assessment Breakdown	%
Coursework	40.00%
End of Module Assessment	60.00%

Assessments

Full Time

Coursework

Assessment Type:	Continuous Assessment	**% of total:**	40
Assessment Date:	n/a	**Outcome addressed:**	1,2,3
Non-Marked:	No		

Assessment Description:
Practical work will be conducted throughout the semester to assess the learner’s skills in terms of design, model and implement a simulation network that will be enable a Security Engineer to reliably perform Incident Response during a compromise. Practical work may involve working in a team.

End of Module Assessment

Assessment Type:	Terminal Exam	**% of total:**	60
Assessment Date:	End-of-Semester	**Outcome addressed:**	1,2,3
Non-Marked:	No		

Assessment Description:
Learners are required to complete a formal end-of-semester examination.

No Workplace Assessment

Reassessment Requirement

Repeat examination
Reassessment of this module will consist of a repeat examination. It is possible that there will also be a requirement to be reassessed in a coursework element.

H9IRSAN: Incident Response and Analytics

Module Workload

Module Target Workload Hours 0 Hours

Workload: Full Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	No Description	1	Every Week	1.00
Tutorial	No Description	1	Every Week	1.00
Independent Learning	No Description	8.5	Every Week	8.50
			Total Weekly Contact Hours	2.00

Module Resources

Recommended Book Resources

Don Murdoch. (2014), Blue Team Handbook: Incident Response Edition: A condensed field guide for the Cyber Security Incident Responder.

P. Cichonski, T. Millar, T. Grance, K. Scarfone. (2012), Computer Security Incident Handling Guide; NIST, National Institute of Standards and Technology; US Department of Commerce.

Richard Bejtlich. (2013), Practice of Network Security Monitoring, Understanding Incident Detection and Response, NoStarch.

Supplementary Book Resources

Laura Chappell. (2012), Wireshark Network Analysis The Official Wireshark Certified Network Analyst Study Guide, 2nd Edition.

Gordon Fyodor Lyon. (2009), Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning Paperback.

This module does not have any article/paper resources

Other Resources

[website], Sans Reading Room,
https://www.sans.org/reading-room/

[website], Forensics,
https://www.sans.org/reading-room/whitep apers/forensics

[website], Incident Handling,
https://www.sans.org/reading-room/whitep apers/incident/

[website], Project Honeynet,
https://www.honeynet.org/

[website], Command Line Kung Fu Blog,
http://blog.commandlinekungfu.com

[website], NSM Wiki,
http://nsmwiki.org/Main_Page

[website], The Incident Handlers Handbook,
https://www.sans.org/reading-room/whitep apers/incident/incident-handlers-handboo k-33901

[website], Security Onion,
https://security-onion-solutions.github. io/security-onion/

[website], Intrusion Detection and Prevention Systems Cheat Sheet: Choosing the Best Solution, Common Misconfigurations, Evasion Techniques, and Recommendations,
https://www.sans.org/reading-room/whitep apers/detection/intrusion-detection-prev ention-systems-cheat-sheet-choosing-solu tion-common-misconfi-36677

Discussion Note:	