2024 / 25

School of Science and Computing

☎ +353 (0)51 302037

✉ Eleanor.Reade@setu.ie

🌐 www.wit.ie/schools/science_computing

Ollscoil
Teicneolaíochta
an Oirdheiscirt

South East
Technological
University

Module Descriptor

Network Forensics (Computing and Mathematics)

Network Forensics (A14030)

Short Title:	Network Forensics		
Department:	Computing and Mathematics		
Credits:	5	**Level:**	Intermediate

Description of Module / Aims

This module aims to provide students with the skills to investigate computer attacks that take place over computer networks. Students gain exposure to penetration testing techniques, incident response techniques and traffic analysis methodologies. The module has a significant practical component where the student will use various analysis tools and techniques to explore the areas listed above.

Programmes

		stage/semester/status
COMP-0129	BSc (Hons) in Applied Computing (International) (WD_KACCM_BI)	3 / 6 / M
COMP-0129	BSc (Hons) in Applied Computing (WD_KACCM_B)	3 / 5 / E
COMP-0129	BSc (Hons) in Applied Computing (WD_KCOMP_B)	3 / 5 / E
COMP-0129	BSc (Hons) in Computer Forensics and Security (WD_KCOFO_B)	3 / 5 / M
COMP-0129	BSc (Hons) in Computer Science (WD_KCMSC_B)	3 / 5 / E

Indicative Content

- Penetration Testing: Probing attacks; Remote to local attacks; User to root attacks
- Incident Response: Live response techniques
- Data Collection
- Data Analysis: Content data; session data; statistical data; alert data
- Report Preparation and Presentation

Learning Outcomes

On successful completion of this module, a student will be able to:

1. Demonstrate attacks remotely on networked computers.
2. Develop an appropriate response strategy to incidents on computer networks.
3. Use appropriate tools to gather network based evidence.
4. Analyse network-based evidence for session, statistical, content and alert data.
5. Produce documentation for an investigation into a network based attack.

Learning and Teaching Methods

- This module will be presented by a combination of lectures and practicals. The lectures will be used to introduce new topics and their related concepts. The practical element allows the student to put into practice the theoretical concepts covered in the lectures.

Learning Modes

Learning Type	F/T Hours	P/T Hours
Lecture	12	
Lab	36	
Independent Learning	87	

Assessment Methods

	Weighting	Outcomes Assessed
Continuous Assessment	100%	
Assignment	50%	1,2,3
Assignment	50%	4,5

Assessment Criteria

<40%: Unable to interpret and describe key concepts of the specific knowledge domain(s). Unable to conduct attack, unable to gather data.

40%–49%: Be able to interpret and describe key concepts of the specific knowledge domain(s). Can only construct basic attack scenarios. Can conduct partial responses to attacks.

50%–59%: Ability to discuss key concepts of the specific knowledge domain and ability to discover and integrate related knowledge in other knowledge domains. Can implement attacks to a moderate level, gather some data and produce some findings.

60%–69%: Be able to solve problems within the specific knowledge domain(s) by experimenting with the appropriate skills and tools. Can implement complex attacks, extract knowledge to recreate accuratly what occurred on the network.

70%–100%: All the above to an excellent level. Be able to analyse and design solutions to a high standard for a range of both complex and unforeseen problems through the use and modification of appropriate skills and tools. Can implement advanced attacks extract and interpret knowledge to recreate accuratly what occurred on the network. Can produce very high quality documentation to accompany the investigation.

Supplementary Material(s)

- Casey, E. *Digital Evidence and Computer Crime.* 3rd. United States: Academic Press, 2011.
- Clark, B. *Rtfm: Red Team Field Manual.* United States: CreateSpace Independent Publishing Platform, 2014.
- Davidoff, S and J Ham. *Network Forensics: Tracking Hackers through Cyberspace.* United States: Prentice Hall, 2012.
- Engebretson, P. *The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy.* United States: Syngress, 2013.
- Jones, K, R Bejtlich and C Rose. *Real Digital Forensics : Computer Security and Incident Response.* New York: Addison-Wesley Professional, 2005.
- Kim, P. *The Hacker Playbook 2: Practical Guide To Penetration Testing.* United States: CreateSpace Independent Publishing Platform, 2015.
- McClure, S, G Kurtz and J Scambray. *Hacking Exposed 7: Network Security Secrets and Solutions.* New York: McGraw-Hill Education, 2012.

Requested Resources

- Computer Lab: BYOD Lab