Module: Penetration Testing 361

Module name:	Penetration Testing 361
Code:	PET361
NQF level:	6
Type:	Speciality – Diploma in Information Technology (Security)
Contact time:	84 hours
Structured time:	10 hours
Self-directed time:	66 hours
Notional hours:	160 hours
Credits:	16
Prerequisites:	SEC261

Purpose

This course teaches students the underlying principles and techniques associated with cybersecurity practices known as penetration testing. Students will acquire the necessary skills for applying penetration testing that include planning reconnaissance, scanning, exploitation, post-exploitation, and results reporting. The course will provide the fundamental information associated with each method exploited and insecurities identified.

Outcomes

Upon successful completion of this module, the student will be able to:

- Demonstrate an informed understanding of basic concepts behind penetration testing processes.
- Demonstrate the ability to perform installations and configurations of the operating system software needed for penetration testing.
- Demonstrate the ability to evaluate and gather the required information for performing penetration testing.
- Demonstrate the ability to evaluate, select and apply appropriate methods, procedures or techniques to mitigate explored vulnerabilities.
- Demonstrate the ability to evaluate, select and apply appropriate methods, procedures, or techniques to perform internal, external, Wi-FI and web application penetration testing.
- Demonstrate an informed understanding of network sniffing and common cybersecurity attacks.
- Demonstrate an understanding of the ethical implications and considerations behind penetration testing.
- Demonstrate the ability to present, communicate and understand penetration testing compliance reports.

Assessment

Assessment is performed using a variety of instruments:

- Continuous evaluation of theoretical work through a written assignment, 3 formative tests and a summative test.

- Continuous evaluation of project work, where the student must design, manage and report on the evaluation of testing methodologies and the selection of an appropriate methodology for a given scenario, justifying the choice made with well-formed arguments and evidence.
- Final assessment through an examination.
- The assignments or projects collectively will count 30% of your class mark.
- All tests will collectively account for 70% of your class mark.
- Your class mark contributes 30% towards your final mark for the subject, while the final assessment accounts for 70% of your final mark.

Teaching and Learning

Learning materials

Prescribed books (EBSCO)

📖 ***Beggs, R.W., 2014. Mastering Kali Linux for advanced penetration testing. Packt Publishing Ltd.***

Additional material

📖 ***Halton, W., Weaver, B., Ansari, J.A., Kotipalli, S.R. and Imran, M.A., 2017. Penetration Testing: A Survival Guide. Packt Publishing Ltd.***

Learning activities

Learning will be facilitated by the lecturer with student centred activities that involve problem-based learning where pupils are presented with challenges that replicate the situation in the real-world environment. This will be achieved through a combination between presentation of theoretical concepts, guided exercises, group work and discussions during the module.

Notional learning hours

Activity	Units	Contact Time	Structured Time	Self-Directed Time
Lecture		76.0		24.0
Formative feedback		4.0		
Project	1	4.0		14.0
Assignment	1			2.0
Test	4		8.0	16.0
Exam	1		2.0	10.0
		84.0	**10.0**	**66.0**

Syllabus

- Installing and configuring the operating system software
- Performing Pre-penetration testing checklist
- Information gathering
- Develop response plans and procedures
- External penetration testing
- Web application penetration testing

- Internal network penetration testing
- Networking Sniffing
- Exploitation vulnerabilities
- Build experience in detecting and containing attacks
- Social engineering
    - PowerShell attack
    - Spear Phishing attack
    - Credential harvester
    - Social engineering toolkit
- Wi-FI penetration testing
    - WEP attacks
    - WPA attacks
    - Bypassing a hidden ESSID
- Brute force attacks
    - Cracking Hashes
    - Web based authentication
    - Brute force RDP
    - Brute force SSH
- Advanced penetration testing
    - Bypassing anti-virus
    - Metasploit Rc Scripts
    - Attacking the domain controller