Module: Ethical Hacking 361

Module name:	Ethical Hacking 361
Code:	EHA361
NQF level:	6
Type:	Speciality – Diploma in Information Technology (Security)
Contact time:	90 hours
Structured time:	10 hours
Self-directed time:	90 hours
Notional hours:	190 hours
Credits:	19
Prerequisites:	PET361

Purpose

This is a comprehensive Ethical Hacking course which contains both Theoretical and Practical Sessions; we'll start with basics of ethical hacking, install the needed software, and perform ethical hacking. From here onwards you'll see everything practical i.e., by analyzing and exploiting different systems such as Network, Applications, Servers and Web applications. So that we don't have any dry theoretical sessions.

Outcomes

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

- Demonstrate an informed understanding of all basic concepts on ethical hacking and networking.
- Demonstrate the ability to evaluate, select and apply appropriate methods, procedures or techniques to install and configure required software for performing ethical hacking.
- Demonstrate the ability to evaluate, select and apply appropriate methods, procedures or techniques to perform attacks on user accounts.
- Demonstrate an informed understanding of the five stages in ethical hacking.
- Demonstrate the ability to identify, analyse and mitigate cybersecurity explored vulnerabilities.
- Demonstrate an understanding of the ethical implications and considerations behind ethical hacking.

Assessment

Assessment is performed using a variety of instruments:

- Continuous evaluation of theoretical work through a written assignment, 4 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)

- ***Najera-Gutierrez, G. and Ansari, J.A., 2018. Web Penetration Testing with Kali Linux: Explore the methods and tools of ethical hacking with Kali Linux. Packt Publishing Ltd.***

Additional material

- ***Broad, J. and Bindner, A., 2013. Hacking with Kali: practical penetration testing techniques. Newnes.***

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		33.0
Formative feedback		10.0		
Project	2	4.0		22.0
Assignment	1			3.0
Test	4		8.0	15.0
Exam	1		2.0	17.0
		90.0	**10.0**	**90.0**

Syllabus

- Introduction to ethical hacking and networking.
- Metasploit Framework
- Hacking Users Accounts with or without Software.
- Other ways to crack user accounts.
- Accessing windows without any password
- Five stages of ethical hacking
- Creating backdoors
- How to create undetectable trojan
- Port Scanning
- SQL Inj. Basics
- Creating and hosting a website

- Server-Side Script creation
- Using Google Dork
- Social Engineering
- Phishing Attack
- Reverse Engineering