CIST 2613 - Ethical Hacking and Penetration Testing (version 201512L)

Course Title	Course Development	Learning Support
Ethical Hacking and Penetration Testing	Standard	No

Course Description

This course teaches students the skills needed to obtain entry-level security specialist jobs. It provides a hands-on introduction to ethical hacking, and penetration testing. It is for individuals who want to enhance their information security skill set and help meet the growing demand for security professionals. Topics include network and computer attacks, footprinting and social engineering, port scanning, enumeration, OS vulnerabilities, hacking web servers, hacking wireless networks, cryptography and network protection systems.

Pre-requisites

Pre-requisites: All Required

CIST 1601 - Information Security Fundamentals (201003L)

Regstr. Co-requisites

Regstr. Co-requisites: None

True Co-requisites

True Co-requisites: None

Course Length

	Lecture Contact Time	Regular Lab Type	Reg. Lab Contact Time	Other Lab Type	Oth. Lab Contact Time	Total Contact Hrs
Contact Hours Per Week	**2 hrs**	**Lab**	**4 hrs**	**N/A**	**0 hrs**	**6 hrs**
Contact Min/Hrs Per Semester	**1500 min**		**3000 min**		**0 min**	**90 hrs**

	Lecture Credit Hours	Lab Credit Hours	Total Credit hours	WLU
Semester Credit Hours	**2**	**2**	**4**	**142.5**

Competencies & Outcomes

Order Description

1 **Network and Computer Attacks**

Order	Description	Learning Domain	Level of Learning
1	Understand the different types of malicious software and what damage they can do	Cognitive	Comprehension
2	Describe the methods of protecting against network attacks	Cognitive	Knowledge
3	Identify physical security attacks and vulnerabilities	Cognitive	Knowledge

2 **Footprinting and Social Engineering**

Order	Description	Learning Domain	Level of Learning
1	Perform footprinting using web tools	Cognitive	Synthesis

2	Conduct competitive intelligence	Cognitive	Application
3	Describe DNS zone transfers	Cognitive	Knowledge
4	Identify the types of social engineering	Cognitive	Knowledge

3 **Port Scanning**

Order	Description	Learning Domain	Level of Learning
1	Describe port scanning and types of port scanning	Cognitive	Knowledge
2	Describe port scanning tools	Cognitive	Knowledge
3	Perform ping sweeps	Cognitive	Synthesis
4	Perform automated security tasks using shell scripts	Cognitive	Synthesis

4 **Enumeration**

Order	Description	Learning Domain	Level of Learning
1	Describe the enumeration step of security testing	Cognitive	Knowledge
2	Enumerate Windows OS targets	Cognitive	Application
3	Enumerate Linux OS targets	Cognitive	Application

5 **OS Vulnerabilities**

Order	Description	Learning Domain	Level of Learning
1	Describe the vulnerabilities of Windows and Linux operating systems	Cognitive	Knowledge
2	Perform vulnerability patching	Cognitive	Synthesis
3	Describe the techniques to harden OS systems	Cognitive	Knowledge

6 **Hacking Web Servers**

Order	Description	Learning Domain	Level of Learning
1	Describe Web applications	Cognitive	Knowledge
2	Explain Web application vulnerabilities	Cognitive	Comprehension
3	Perform Web server attack using security tools	Cognitive	Synthesis

7 **Hacking Wireless Networks**

Order	Description	Learning Domain	Level of Learning
1	Understand wireless technologies	Cognitive	Comprehension
2	Describe wireless networking standards	Cognitive	Comprehension

3	Describe the process of wireless authentication	Cognitive	Comprehension
4	Perform wireless hacking using security tools	Cognitive	Synthesis

8 **Cryptography**

Order	Description	Learning Domain	Level of Learning
1	Understand the principals of cryptography	Cognitive	Comprehension
2	Describe symmetric and asymmetric encryption algorithms	Cognitive	Comprehension
3	Perform cryptosystem attacks	Cognitive	Synthesis