Course number and name:	**CS 03551: Advanced Cyber Security Principles & Applications**
Credits and contact hours:	3 credits / 3 contact hours
Instructor's or course coordinator's name:	Fred Stinchcombe
Text book, title, author, and year:	Beggs, Robert W. and Vijay Kumar Velu. *Mastering Kali Linux for Advanced Penetration Testing*. Packt, 2019 .

Specific course information

Catalog description: This graduate course examines the principles of cyber security and will introduce students to a wide range of security activities, methodologies, and procedures. The topics covered in the course include fundamental concepts of computer security: threats, attacks, and assets; principles of cryptography: encryption, decryption, authentication, and non-repudiation; software security and trusted systems: developing secure software, buffer overflow attacks, operating security issues, trusted systems; network security: intrusion detection, firewalls and intrusion prevention systems, distributed denial-of-service attacks, malicious software, protocols for network security; as well as other topics.

Prerequisites:

Type of Course: ☐ Required ☒ Elective ☐ Selected Elective

Specific goals for the course:

1. Students will develop an understanding of information security architecture and strategies.
2. Students will explore and utilize the wide range of Cyber Security Tools available for red teams
3. Students will explore the dynamic landscape of information security and develop the ability to identify and prioritise information assets.
4. Students will understand the concept of the cyber kill chain and how to implement the stages through the use of appropriate tools

Required List of Topics to Be Covered:

1. Basic principles of reconnaissance
2. OSINT
3. Online resources and dark web searches
4. Obtaining user information

5. Profiling user for password lists
6. Comprehensive reconnaissance of applications
7. External and internal infrastructures
8. Enumeration of internal hosts
9. Social engineering attack methods
10. Wireless Recon
11. Web Application hacking methodology
12. Vulnerability Scanning
13. Backdoor executables
14. Cross site Scripting
15. BEEF
16. Bypassing Security access controls
17. Privilege escalation
18. Post-exploitation tools
19. Pivoting and port forwarding
20. Common escalation methodology
21. Credential harvesting