Course Code	Course Title
COMP 4632	**Practicing Cybersecurity: Attacks and Counter-measures**

Course Description

This course equips students with cybersecurity knowledge and current IT practices on security risk management. Through hands-on laboratory sessions, students will understand existing IT security issues, learn how to assess IT security risks, and conduct experiments on ethical hacking. They will practice system attack and defense strategies using security tools, so as to gain practical experience to become a cybersecurity professional. The course covers current security trends, industrial practices on IT security, design requirements for secure web and mobile applications, security assessment, risk analysis and risk management. Knowledge in web programming and database administration is not essential but a plus. Prerequisite(s): COMP 2012 OR COMP 2012H; Corequisite(s): COMP 3511

List of Topics

Class Content and Descriptions
Basic Concept on IT Security and setup of Virtualization Environment (Lecture): Briefing on CyberSecurity practices, Threats and Vulnerabilities (Lab): Setup of ESXi server and walk through of vSphere client and VM environment. Setup of Kali Linux and Windows 10 Victim Guest OS.
OS Security and Virtualization (Lecture): Network basis, Network architecture and security architecture, Virtualization, Virtualization security (Lab): Setup Linux and Wiresharks lab environment, virtual network. Perform WiFi analysis, WiFi exploits and WiFI cracking
Network Basics (Lecture): DNS, LAN and WAN, Directory services and Database security, PKI, SSL TLS, Secure Protocol, Heartbleed and POODLE (Lab): Setup Web and FTP services, DNS services, database services in cloud instances within the AWS environment.
Network Security (Lecture): Network attack, scanning, sniffing, vulnerability scanning, Denial of Service attacks, email security, phishing (Lab): Perform network scanning (nmap), vulnerability scanning (nessus), Open Source Intelligence Collection including DNS information collection.

Web Application Programming (Lecture): Web Protocol, PHP, Javascript, SQL query and web authentication (Lab): Develop and deploy a web site through the use of CSS, PHP and Javascript. Connect PHP web site to the database and then setup authentication component to the web site.
Web Application Hacking (Lecture): OWASP top 3/10 attack methods including SQL injection, XSS, CSRF (Lab): Perform web attack using different kinds of web attack methods web session management attack, injection attack, Cross-site scripting and CSRF attack
Operating System Security (Lecture): System and Kernel Attack, Patch Management, Trusted System Security (Lab) Perform system exploitation using Metasploit, existing exploit scripts and payloads.
IAM, Authentication and Authorization (Lecture): Authentication, Authorization, Password Scheme, Federated Authentication (Lab) Perform password cracking, password dumping, and implement 2-factor authentication into the web site setup in previous weeks.
Application Security (Lecture): Application security threats, Secure programming life cycle, Buffer Overflow, Application firewall, secure code review and security assessment concept, malware and virus (Lab) Perform software exploitation, understand and use various debug tools such as gdb, Ghidra and compose buffer overflow code.
Secure Infrastructure Design (Lecture): Network defense mechanism, Firewall, IDS, Anti-DDoS, Honeypot (Lab): Setup Firewall, VPN and Snort IDS, SSH Tunnel
Incident Response and Computer Forensics (Lecture): Incident Response, Computer Crime, Forensics Investigation and Compliance (Lab): Setup big data platform environment (ElasticSearch) for performing log analysis and attack tracing
Advanced Topics on Security (Lecture): (Lab): Project presentation
3 hrs Open book Practical Examination (10:30 - 13:30)

Textbook

N/A

Reference books

- Bosworth S., Kabay M. and Whyne E. (2014). Computer Security Handbook. Sixth Edition, Volume 1. John Wiley & Sons, Inc.
- Donaldson S., Siegel S., Williams C. and Aslam A. (2014). Enterprise Cybersecurity, How to build a successful cyberdefense program against advanced threats. Apress Open
- Kurose J. and Ross K. (2013). Computer Networking, A Top-Down Approach. Sixth Edition. Addison-Wesley
- Joseph Migga Kizza (2015). Guide to Computer Network Security. Third Edition. Springer-Verlag London
- OWASP (2017). OWASP Testing Guide 4.0
- Umesh Hodeghatta Rao and Nayak U. (2014). The InfoSec Handbook – An Introduction to Information Security. Apress Open
- National Institute of Standards and Technology (2014). Framework for Improving Critical Infrastructure Cybersecurity. Version 1.0.
- Stallings, W. (2011). Cryptography and Network Security, Principles and Practice. Fifth Edition. Prentice Hall.
- Stallings, W. (2012). Computer Security Principles and Practice. Second Edition. Prentice Hall.

Grading Scheme

In class course work	30% (3 marks per week)
Attendance	10% (1 mark per week)
3 Assignments (2 written assignments and one group presentation)	30% (5 marks, 5 marks, 20 marks)
1 Test	30%
Total	100%

Course Intended Learning Outcomes

On successful completion of this course, students are expected to be able to:
(1) Understand the current security threat and future trend of IT security industry
(2) Design and develop network and server with security features
(3) Incorporate best security practices in IT infrastructure (such as ISO 27000 series, OWASP Top 10 risks)
(4) Apply Information security governance and risk management to real life scenario
(5) Perform auditing of information systems
(6) Set up ethical hacking and security testing/assessment tools
(7) Launch exploits to network and system environment

Assessment Rubric

N/A