SILVER OAK UNIVERSITY
EDUCATION TO INNOVATION

COLLEGE OF SCIENCE					
Program	Master of Science		Branch/Spec.	Cyber Security & Digital Forensics	
Semester	III		Version	1.0	
Effective from Academic Year		2020 - 21	Effective for the batch Admitted in		June 2020
Subject code		Subject Name	Security Monitoring		

Pre-requisites:

- Network security and working sensors.
- Fundamentals of IPS and IDS
- Understanding of Snort and Suricata
- Log analysis for Firewalls

Learning Outcome:

After studying this course, you should be able to:

- Identify some of the factors driving the need for network security
- Identify and classify particular examples of attacks
- Define the terms vulnerability, threat and attack
- Identify physical points of vulnerability in simple networks

Theory syllabus

Unit	Content	Hrs
1	**Security Monitoring fundamentals:** What is Security Operations, Finding the sweet spot, Security and Control, Security Goals, Reliability vs Security, Typical Security Flaws, basics of SOC infrastructure.	10
2	**Log management:** Computer Security Log Management, Log Management Infrastructure, Log Management Planning, Log Management Operational Process	9
3	**Security Information & Event Management:** Introduction to SIEM, SIEM Architecture, Logs and Events, Understanding logs, various formats, Log Baselining, Aggregation and normalization, Event Collection and Event Correlation, Correlation Rules	10
4	**Incident Response Plan and handling steps:** Purpose of Incident Response Plan, Requirements of Incident Response Plan, Preparation, Incident Recording, Initial Response, Communicating the Incident, Containment, Formulating a Response Strategy, Incident Classification, Incident Investigation, Data Collection, Forensic Analysis, Evidence Protection, Notify External Agencies, Eradication, Systems Recovery, Incident Documentation, Incident Damage and Cost Assessment, Review and Update the Response Policies	11

Practical content

- Perform Installation deployment of SIEM systems like Qradar, Splunk, Arcsight.

- Perform operations to collect logs at centralized location using logger.
- Perform operations with smart connectors to manage IT assets.
- Perform security operation/investigations on different types of security events.
- Perform threat hunting using Splunk.
- Perform vulnerability management using SIEM.
- Perform orchestration of common security related events and investigations.
- Perform incidence recovery for threat mitigation using SIEM.

Reference Books	
1	Security Metrics, A Beginner's Guide – Caroline Wong
2	The Computer Incident Response Planning Handbook – N.K. McCarthy, Matthew Tod, Jeff Klaben
3	The Practice of Network Security Monitoring: Understanding Incident Detection and Response By Richard Bejtlich
4	Information Assurance Handbook: Effective Computer Security and Risk Management Strategies – Corey Schou, Steven Hernandez

COLLEGE OF SCIENCE					
Program	Master of Science		Branch/Spec.	Cyber Security & Digital Forensics	
Semester	III		Version	1.0	
Effective from Academic Year		2020 - 21	Effective for the batch Admitted in		June 2020
Subject code		Subject Name	Cyber Crime Investigation & Forensic		

Pre-requisites:

- Basic knowledge of system and mobile devices
- Social Networking platforms
- Types of web application functionality

Learning outcome

Upon Successful completion of this course, student will be able

- To extend the students' knowledge of Cyber Crimes & IT ACT.
- To enhance their expertise in Cyber Crime Investigation and methodologies.
- To carry out real life cyber forensics assignments.

Theory syllabus

Unit	Content	Hrs
1	**Introduction to Cyber Crime Investigation & Cyber Forensics** Cyber Crime Investigation - Cyber Warfare, Terrorism & Social Networking - Cyber Forensics and Incident Handling - Case Study - Cyber Forensic Basics - Storage Fundamentals - File System Concepts	6
2	**Investigating Real World Cyber Crimes** Investigating Social Media Profile Impersonation cases - Phishing Cases - Data Theft Cases - Corporate Espionage Cases - Email Fraud Cases - Credit Card Fraud Cases - Cyber Pornography Cases - Denial of Service Attacks Cases - Cyber defamation Cases - Real Life Case Studies	9
3	**IT ACT, Offenses and Penalties** Offences under the Information and Technology Act 2000 - Penalty and adjudication - Punishments for contraventions under the Information Technology Act 2000 (Case Laws, Rules and recent judicial pronouncements to be discussed) - Limitations of Cyber Law	5
4	**Data Recovery Tools, Process, and Ethics & Cyber Forensics Investigation** Gathering Evidence- Precautions, Preserving and safely handling original media for its admissibility - Document a Chain of Custody and its importance - Complete time line analysis of computer files based on file creation - file modification and file access - Data Protection and Privacy. Introduction to Cyber Forensic Investigation - Investigation Tools – eDiscovery - Digital Evidence Collection - Evidence Preservation - E-Mail Investigation - Encryption and Decryption methods - Search and Seizure of Computers - Work on open Source, Commercial tools and Cyber range	19

Practical content

- Performing method to create image of hard disk and removable storage media.
- Performing Deleted File Recovery & Formatted Partition Recovery.
- Performing Recovery of Internet Usage Data
- Performing forensic investigation using Encase Forensic Edition.
- Working with Forensic Toolkit.
- Performing tracking on E-Mail, IP Tracking, E-Mail Recovery
- Password Cracking, Cracking with GPU Systems (Hashcat).

Reference Books

1	International domain name law: ICANN and the UDRP. Oxford: Hart Publishing by Lindsay D.
2	Cyber Laws. New Delhi: Ane Books Pvt. Ltd by Sharma J. P & Kanojia S.
3	Cyber Laws. Universal Law Publishing by Duggal P.
4	Law relating to computers, internet and e-commerce: A guide to Cyber Laws and the IT Act, 2000 with rules, regulations and notifications (2nd ed.). Delhi: Universal Law Publishing Co. by Kamath N.
5	Investigating computer- related crime a handbook for corporate investigators. Boca Raton Stephenson P.R. & Gilbert K.
6	Cyber Law: The Law of the Internet and Information Technology. Pearson Education by Craig B
7	Incident response & computer forensics (2nd ed.) McGraw-Hill Companies by Prosise C. & Mandia K.

COLLEGE OF SCIENCE					
Program	Master of Science		Branch/Spec.	Cyber Security & Digital Forensics	
Semester	III		Version	1.0	
Effective from Academic Year		2020 - 21	Effective for the batch Admitted in		June 2020
Subject code		Subject Name	Elective (Metasploit Framework-II)		

Pre-requisites:

- Be able to download and install all the free software and tools needed to practice
- A strong work ethic, willingness to learn and plenty of excitement about the back door of the digital world
- Nothing else! It's just you, your computer and your ambition to get started.

Learning outcome

- Persist your connection in the compromised system
- Crack the administrator password
- Capture the keystrokes of the compromised system
- Learn What is Pivoting? and pivot from the victim system to own every device on the network
- Learn what is BeEF? and how to use it
- Hook any user browser with BeEF control panel
- Launch the best BeEF project modules in the target browser
- Full control Windows OS of the hooked browser
- Launch BeEF over WAN network
- Learn the theory behind getting a reverse connection over WAN network
- Launch all the previous attacks over WAN network

Theory syllabus

Unit	Content	Hrs
1	**Meterpreter-2** Setting up multiple communication channels with the target, Meterpreter anti-forensics, the get-desktop and keystroke sniffing, Meterpreter resource scripts, Meterpreter timeout control, Meterpreter Sleep Control, Meterpreter transports, Interacting with the registry, Meterpreter API and mixins, Injecting VNC server remotely, Enabling remote Desktop	10
2	**Server Side Exploitation** Exploiting a Linux server, Exploiting a Windows machine, Exploiting Common services	8
3	**Client Side Exploitation** Bypassing antivirus and IDS/IPS, Human interface device attacks, HTA attack, Backdooring executables using a MITM attack, Creating a Linux trojan, File format based Exploitation-PDF and Word, Creating an Android backdoor	8

4	**Wireless Network penetration Testing** Metasploit and wireless, understanding an evil twin attack, Configuring karmetasploit, Wireless MITM attacks, SMB relay attacks	10
Practical content		
• Meterpreter anti-forensics • The getdesktop and keystroke sniffing • Interacting with the registry • Meterpreter API and mixins • Injecting VNC server remotely • Enabling remote Desktop • Exploiting a Linux server • Exploiting a Windows machine • Exploiting Common services • Bypassing antivirus and IDS/IPS		
Reference Books		
1	Metasploit Penetration Testing Cookbook-Packet Publishing	
2	Metasploit Revealed _ Secrets of the Expert Pentester - Build your Defense against Complex Attacks-Packet Publishing	

COLLEGE OF SCIENCE					
Program	Master of Science		Branch/Spec.	Cyber Security & Digital Forensics	
Semester	III		Version	1.0	
Effective from Academic Year		2020 - 21	Effective for the batch Admitted in		June 2020
Subject code		Subject Name	Elective (Cloud Security)		

Pre-requisites:

Knowledge Network terminologies
Configuration
Protocols
Wireless networks
Cloud fundamentals

Learning Outcome:

After successful completion of the course students should be able to

Develop cloud-based applications.
Deploy the application on real cloud.
To analyse and trouble shoot the problems while deploying application on cloud.
Use LAMP technology for developing application using cloud.
Use public cloud like IBM Bluemix, Amazon AWS, for developing an application.
Performing vulnerability assessment and penetration testing on cloud.
Performing configuration review on different clouds.
Enhance knowledge of cloud security compliance management.

Theory syllabus

Unit	Content	Hrs
1	**Introduction to Cloud Computing** Cloud Computing definition, private, public and hybrid cloud. Cloud types; IaaS, PaaS, SaaS. Benefits and challenges of cloud computing, public vs private clouds, role of virtualization in enabling the cloud; Business Agility: Benefits and challenges to Cloud architecture. Application availability, performance, security and disaster recovery; next generation Cloud Applications	10
2	**Cloud Application Architecture and security** Technologies and the processes required when deploying web services - Deploying a web service from inside and outside a cloud architecture - advantages and disadvantages.	9
3	**Implementing Cloud Application, Services and security** Reliability, availability and security of services deployed from the cloud. Performance and scalability of services - Cloud Economics: Cloud Computing infrastructures available for implementing loud based services. Cloud security controls, Dimensions of cloud security, Cloud Vulnerability and Penetration Testing, Data security, Encryption, Compliance.	11

4	**Cloud Application Development & IT Model & Importance of Cloud Technology in Corporates** Service creation environments to develop cloud-based applications. Development environments for service development; Amazon, Azure, Google App. Applicability of laws to data stored outside the nation's boundary**.** Economics of choosing a Cloud platform for an organization - Based on application requirements, economic constraints and business needs - Discuss industry cases including open sources.	11

Practical content
Building and Deploying JAVA/NODE.js based application on public cloud-based application Perform Blackbox penetration testing on Cloud applications to get an access to internal cloud resources. Performing cloud configuration review on a public cloud platform Performing vulnerability assessment on EC2 container using Nessus. Performing vulnerability assessment on Docker using Nessus. Performing signature rapping attacks and side channel attacks in cloud-based applications. Security Controls in Cloud and Tools used for Security Control Implementation

Reference Books	
1	Computing: Implementation, Management, and Security. CRC Press - Rittinghouse, J.W. & Ransome, J.F.Cloud
2	Cryptography & Network Security. Paperback – Stallings
3	Cloud Computing Security: Foundations and Challenges. CRC Press - Vacca, J.
4	The Basics Of Cloud Computing: Understanding The Fundamentals Of Cloud Computing In Theory And Practice. Syngress, Elsevier - Rountree, D. & Castrillo, I.

CSF505 – Mini Project – 4 Credits