SILVER OAK UNIVERSITY

Silver Oak College of Computer Application
Master of Science Cyber Security & Digital Forensics
Course Name: Practical-2 (Security Monitoring)
Course Code: 1040147204
Semester: 3rd

Prerequisite: Network security and working sensors, Fundamentals of IPS and IDS, Understanding of Snort and Suricata, Log analysis for Firewalls

Course Objective: The Security Monitoring is part of the Security Operation Center where a process is set to detect, analyze, and respond to cyber security incidents using a combination of technology and tools and a strong set of processes.

Teaching Scheme:

Teaching Scheme				
L	T	P	Contact Hours	Credit
0	0	8	8	4

List of Experiments: **Total Hours: 112**

Sr. No.	Practical Name
1.	Perform searches in Splunk using lookup tables to enrich and correlate data.
2.	Design and build interactive dashboards and panels for data visualization in Splunk.
3.	Learn to create basic charts to visualize data trends and patterns in Splunk.
4.	Use Splunk's Add Data Wizard to upload and index new data sources.
5.	Configure field lookups to map external data fields into Splunk searches.
6.	Install and configure Wazuh for monitoring and security management.
7.	Collect and analyze logs from various sources using Wazuh.
8.	Implement File Integrity Monitoring and Intrusion Detection with Wazuh.
9.	Use Wazuh to identify and assess vulnerabilities in the system.
10.	Install Snort and use shell commands for configuration and management.
11.	Create and test Snort rules to detect various network activities.
12.	Analyze network packets from PCAP files using Snort.
13.	Implement Snort rules to reject or drop malicious packets.

14.	Use advanced search commands in Splunk for complex data queries.
15.	Use Wazuh to handle and respond to security incidents.
16.	Implement compliance monitoring with Wazuh to meet regulatory requirements.
17.	Implement centralized log collection to manage logs effectively.
18.	Practice log analysis techniques and automated correlation for threat detection.
19.	Utilize log data for threat hunting and forensic analysis.
20.	Explore User and Entity Behavior Analytics (UEBA) for advanced monitoring.

Course Outcomes:

Sr. No.	CO Statement
CO-1	Installation and Deployment of SIEM Systems
CO-2	Centralized Log Management and IT Asset Management
CO-3	Security Operations, Threat Hunting, and Vulnerability Management
CO-4	Security Event Orchestration and Incident Recovery

Teaching & Learning Methodology:

1. Design Thinking
2. Cooperative-based Learning
3. Competency-based Learning

Books Recommended:

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

CO-PO-PSO MATRIX:

Co. No	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PSO1	PSO2
CO-1	2	3	3	2	2			2	2
CO-2	2	3	3	2		1		2	3
CO-3	2	3	2	3	2			3	3

CO-4	3	3		2		2		3	3