SILVER OAK UNIVERSITY
EDUCATION TO INNOVATION

COLLEGE OF SCIENCE

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

Pre-requisites:

- Basics of network
- Basics of working of VPN
- Network sniffing and security
- Wireless protocols

Learning Outcome:

Upon successful completion of this course, student will be able to learn

- Learn networking concepts and enhance their knowledge of different network devices.
- Learn and apply different types of network and wireless attacks and their countermeasures
- Executing vulnerability assessment and penetration testing on IT Landscape of organization.
- Preparing VAPT reports.
- Enhance their skills on Patch Management of IT Organization.

Theory syllabus

Unit	Content	Hrs
1	**Introduction to Computer Network:** Types of networks, IP Address, NAT , IP Subnets, DHCP Server, Ports, DNS, Proxy Servers, Virtual Private Networks, DNS Server, OSI and TCP IP Model, Routers , Switches, Endpoint solutions, Access Directory, TOR Network.	9
2	**Types of Networks & policy:** Networking Devices (Layer1,2,3) - Different types of network layer attacks–Firewall (ACL, Packet Filtering, DMZ, Alerts and Audit Trails) – IDS,IPS and its types (Signature based, Anomaly based, Policy based, Honeypot based).	8
3	**VPNS:** VPN and its types –Tunneling Protocols – Tunnel and Transport Mode –Authentication Header Encapsulation Security Payload (ESP)- IPSEC Protocol Suite – IKE PHASE 1, II – Generic Routing Encapsulation(GRE). Implementation of VPNs.	8
4	**Network & Wireless Attacks :** Network Sniffing, Wireshark, packet analysis, display and capture filters, Ettercap, DNS Poisoning, ARP Poisoning, Denial of services, Vulnerability scanning, Nessus, Network Policies, Open VAS, Sparta, Network Scanning Report Generation, System hardening, secure system configurations, SSL Striping, Setup network IDS/IPS, Router attacks, VPN Pen-testing, VOIP Pen-testing, Protocols, MAC Filtering, Packet Encryption, Packet Sniffing, Types of authentication, ARP Replay attack, Fake Authentication Attack, De authentication, Attacks on WEP , WPA and WPA-2 Encryption, fake hotspots, evil twin attack, fluxion framework	15

Practical content

- To Implement VPN server, Configuration of VPN server.

- To Implement TOR Network and Honeypots on windows server 2012.
- Hands-on practice on Network Sniffing using Wireshark, Ettercap and perform man in the middle attack.
- To perform Packet analysis, display and capture filters using Wireshark to identify the sensitive information.
- To execute DNS Poisoning, ARP Poisoning attacks using Ettercap.
- Using Vulnerability scanners like Nessus Open VAS, Sparta. Configuring it for different network types and executing vulnerability scans in networks.
- To implement Vulnerability assessment using Nessus and Nmap.
- To Create & Implement Nessus and Nmap policies for Security Assessment.
- To perform exploitation on different local and remote exploits based on CVEs using Metasploit.
- To Performing WPA and WPA-2 Attacks for wireless networks using Kali Linux
- Creating fake hotspots and executing evil twin attacks.

Reference Books	
1	Network Security, Private communication in public world (2nd Ed.). PHI - Kaufman, C., Perlman, R., & Speciner, M.
2	Network Security. Wiley - Perez, Andre.
3	Cryptography and Network Security: Principles and Practice (5th Ed.). Prentice Hall - Stallings, W.
4	Network Attacks and Exploitation: A Framework. Wiley - Monte, M.

OLLEGE OF SCIENCE

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

Pre-requisites:

- Fundamentals of Android and iOS architecture
- Mobile rooting and Jailbreaking
- Understanding of IPA and APK

Learning Outcome:

Upon Successful completion of this course, student will be able to

- Fundamentals of Android and IOS Applications.
- Mobile application security controls.
- Security measures in the sphere of native, mobile web, and hybrid applications.
- Vulnerability Assessment & Penetration Testing on Mobile applications
- Enhance Compliance Management based on Mobile OWASP Top 10 .

Theory syllabus

Unit	Content	Hrs
1	**Introduction to Android Applications and Mobile App Security:** History of Android, Understanding Android Hardware and Software Architecture, Understanding Android Security Model. Understanding Android Permission Model for Application Security, Sandboxing, Codesigning, Encryption, rooting Devices, Understanding APK Understanding Directories and Files on an APK	9
2	**Introduction to IOS & IPA Applications:** History of iOS, Understanding iOS Hardware and Software Architecture, Understanding iOS Security Model, Understanding iOS Permission Model for Application Security, Sandboxing, Codesigning, Keychain and Encryption, Jailbreaking Devices, Understanding IPA Understanding Directories and Files on an IPA	11
3	**Mobile Application Attacks 1:** Setting up Mobile App Pentesting Environment, Interact with the Devices, Starting with Drozer, Understanding AndroidManifest.xml, Configuring, Burp and Traffic Interception, Traffic Interception Bypass, Weak Server Side Controls, Insecure Data Storage, Insufficient Transport Layer Protection, Unintended Data Leakage, Poor Authentication & Authorization	10
4	**Mobile Application Attacks 2:** Broken Cryptography, Client Side Injections, Security Decisions via Untrusted Input, Improper Session Handling, Lack of Binary Protection, Exploiting Debuggable Applications, Developer Backdoor, Location spoofing to download location restricted apps, Configuring Live Device for Penetration Testing, Mitigation Approach for all Vulnerabilities.	9

Practical content

- Setting up Mobile App Pentesting Environment, interact with the Devices, Starting with Drozer
- Configuring, Burp and Traffic Interception of Mobile Applications between client and server
- Configuring Live Device for Penetration Testing, Mitigation Approach for all Vulnerabilities.
- Performing static Analysis of Mobile Application using MOBSF

• Perform the jailbreak/Root the Android phone and get admin level Privilege by using tools such as Superoneclick, superboot. • Performing Cross-application scripting error in Android Browser which leads to hacking the devices. • Detect application communication vulnerabilities and perform exploitation using ComDroid. • Perform Jailbreaking on iOS Devices. • Unlock the iPhone using tools such as iphonesimfree and anySIM. • Perform a method to send Malicious Payload to the victims iPhone and check whether you can take over the control the victim’s phone. • Perform Man-in-the-Middle attack by intercepting the Wireless parameter of iPhone on wireless network. • Perform social engineering Attack method and send the malicious link and SMS tricks which contains Malicious web page. • Performing dynamic analysis to find API/Web services vulnerabilities. • Performing reverse engineering on android applications • Performing network communication attacks in Android and iOS. • Performing authentication and session management attacks.	
Reference Books	
1	Mobile device security: A comprehensive guide to securing your information in a moving world. Boca Raton, FL: Auerbach Publications - Fried, S.
2	The web application hacker’s handbook: Discovering and exploiting security flaws (2nd ed.). Indianapolis, IN: Wiley, John & Sons - Stuttard, D. & Pinto, M.
3	Mobile application security. New York: McGraw-Hill Companies - Dwivedi, H., Clark, C., & Thiel, D.

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

Pre-requisites:

- NA

Learning Outcome:

A student passing this module should be able to:

- Provide holistic approach to organization information security.
- Define risk assessment and management process for organization.
- Reformulate and use practical, conceptual and technological understanding to create security roles, procedures and management structures appropriate for an organization.
- Develop an appropriate business continuity and disaster recovery plan for an organization.
- Enhance knowledge of cyber security frameworks like ISO270001, PCI, CIS, NIST.

Theory syllabus

Unit	Content	Hrs
1	**ISMS – ISO27001** & **Audit Planning** Introduction to ISO27001, Fundamental principles of information security, ISO/IEC 27001 certification process, Information Security Management System (ISMS), Fundamental audit concepts and principles, Audit approach based on evidence and on risk, Preparation of an ISO/IEC 27001 certification audit, ISMS documentation audit, Conducting an opening meeting	**12**
2	**ISMS Audit – Implementation** Communication during the audit, Audit procedures: observation, document review, interview, sampling techniques, technical verification, corroboration and evaluation, Audit test plans, Formulation of audit findings, Documenting nonconformities	**10**
3	**ISMS Audit – Assurance** Audit documentation, Quality review, Conducting a closing meeting and conclusion of an ISO/IEC 27001 audit, Evaluation of corrective action plans, ISO/IEC 27001 Surveillance audit, internal audit management program	**10**
4	**Other Compliances – PCI DSS** Security Management Process, Risk Analysis Risk Management, Information System Activity Review, Assigned Security Responsibility, Authorization and/or Supervision, Termination Procedures, Access Authorization, Access Establishment and Modification, Protection from Malicious Software, Log-in Monitoring, Password Management, Response and Reporting, Contingency Plan Evaluation, Facility Access Control and Validation Procedures, Unique User Identification, Emergency Access Procedure, Automatic Logoff Encryption and Decryption, Audit Controls, Data Integrity, Person or Entity Authentication, Integrity Controls Encryption	**10**

Reference Books	
1	Implementing Information Security Based on ISO 27001/ISO 27002: A Management Guide (2nd Ed.). Van Haren Publishing - Calder, A.
2	Implementing the ISO / IEC 27001 Information Security Management System Standard. Artech House Publishers - Humphreys, E
3	An Introduction to Information Security and ISO 27001: A Pocket Guide. IT Governance Publishing - Watkins, S. G.
4	Information Systems Security: Security Management, Metrics, Frameworks and Best Practices. Wiley - Godbole, N.

COLLEGE OF SCIENCE

Program	Master of Science	Branch/Spec.	Cyber Security & Digital forensics	
Semester	II	Version	1.0	
Effective from Academic Year		2020 - 21	Effective for the batch Admitted in	June 2020
Subject code		Subject Name	Metasploit Framework-I	

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:

- Learn installing Kali Linux as VM & your main OS
- Learn preparing your penetration testing lab
- Learn Linux commands and how to interact with Terminal
- Learn Linux basics
- Gather information from any target
- Learn how to use Nmap to gather information
- Learn how to use Zenmap to gather information
- Learn what is Metasploit
- Learn using Metasploit like professionals
- Learn using Msfvenom
- Learn creating an undetectable payload
- Learn combining your payload with any type of file
- Learn creating an unsuspicious and undetectable backdoor
- Learn spoofing the backdoor extention
- Learn interacting with the compromised system via Meterpreter command line
- Escalate your privileges

Theory syllabus

Unit	Content	Hrs
1	**Introduction to Metasploit** Importance of Penetration Testing, Vulnerability Assessment vs Penetration Testing, the need for a penetration testing framework, Installing Metasploit on Windows, Installing Metasploit on Linux	**9**
2	**Metasploit Components** Anatomy and Structure of Metasploit, Metasploit Components, Understanding the MSFconsole, Variables in Metasploit	**10**
3	**Information Gathering with Metasploit** Enumerating protocols, Password sniffing, Advanced recon with Shodan, Passive Info. gathering, Active info. gathering, Port scanning- The Nmap way, Host discovery with ARP Sweep, UDP Service Sweeper, SMB scanning and enumeration, Detecting SSH versions, FTP scanning, SMTP enumeration, SNMP Enumeration, HTTP Scanning, WinRM scanning and brute forcing	**10**
4	**Meterpreter-1** What is Meterpreter? Meterpreter core commands, Meterpreter file system commands, Meterpreter networking commands, Meterpreter system commands, Dumping the Hashes and cracking with JTR(John the ripper), Shell command, Privilege escalation	**10**

Practical content	
• Dumping the Hashes and cracking with JTR(John the ripper) • Shell command • Privilege escalation • Metasploit Macro Exploits • Exploiting a Windows machine • Social engineering with Metasploit • Browser Autopwn	
Reference Books	
1	Metasploit Penetration Testing Cookbook-Packt Publishing
2	Metasploit Revealed _ Secrets of the Expert Pentester - Build your Defense against Complex Attacks-Packt Publishing

Important Note: Practicals might be subject to change as per technology and methodology changes in real world.