Information Security

B. Sc. (Information Technology)		**Semester – VI**	
Course Name: Information Security		**Course Code: USIT602**	
Periods per week (1 Period is 50 minutes)		**5**	
Credits		**2**	
		Hours	**Marks**
Evaluation System	**Theory Examination**	**2½**	**75**
	Internal	**--**	**25**

Course Objective:

- To understand the importance of Information protection
- To learn current best practices in storage capacity
- To understand the fundamental security aspects of network devices and learn techniques for hardening network devices against attacks.
- To familiarize Intrusion Detection and Prevention Systems, Voice over IP(VoIP) and PBX security
- To understand the security considerations for virtual machines and security aspects of cloud computing

Unit	Details	Lectures
I	**Information Security Overview**: The Importance of Information Protection, The Evolution of Information Security, Justifying Security Investment, Security Methodology, How to Build a Security Program, The Impossible Job, The Weakest Link, Strategy and Tactics, Business Processes vs. Technical Controls. **Risk Analysis**: Threat Definition, Types of Attacks, Risk Analysis, Secure Design Principles: The CIA Triad and Other Models, Defense Models, Zones of Trust, Best Practices for Network Defense.	**12**
II	**Authentication and Authorization**: Authentication, Authorization **Encryption**: A Brief History of Encryption, Symmetric-Key Cryptography, Public Key Cryptography, Public Key Infrastructure. **Storage Security**: Storage Security Evolution, Modern Storage Security, Risk Remediation, Best Practices. **Database Security**: General Database Security Concepts, Understanding Database Security Layers, Understanding Database- Level Security, Using Application Security, Database Backup and Recovery, Keeping Your Servers Up to Date, Database Auditing and Monitoring.	**12**
III	**Secure Network Design**: Introduction to Secure Network Design, Performance, Availability, Security. **Network Device Security**: Switch and Router Basics, Network Hardening. **Firewalls**: Overview, The Evolution of Firewalls, Core Firewall Functions, Additional Firewall Capabilities, Firewall Design. **Wireless Network Security**: Radio Frequency Security Basics, Data-Link Layer Wireless Security Features, Flaws, and Threats, Wireless Vulnerabilities and Mitigations, Wireless Network Hardening Practices	**12**

	and Recommendations, Wireless Intrusion Detection and Prevention, Wireless Network Positioning and Secure Gateways.	
IV	**Intrusion Detection and Prevention Systems:** IDS Concepts, IDS Types and Detection Models, IDS Features, IDS Deployment Considerations, Security Information and Event Management (SIEM). Voice over IP (VoIP) and PBX Security: Background, VoIP Components, VoIP Vulnerabilities and Countermeasures, PBX, TEM: Telecom Expense Management. **Operating System Security Models**: Operating System Models, Classic Security Models, Reference Monitor, Trustworthy Computing, International Standards for Operating System Security.	**12**
V	**Virtual Machines and Cloud Computing**: Virtual Machines, Cloud Computing. **Secure Application Design**: Secure Development Lifecycle, Application Security Practices, Web Application Security, Client Application Security, Remote Administration Security. **Physical Security:** Classification of Assets, Physical Vulnerability Assessment, Choosing Site Location for Security, **Securing Assets**: Locks and Entry Controls, Physical Intrusion Detection.	**12**

Books and References:

Sr. No.	**Title**	**Author/s**	**Publisher**	**Edition**	**Year**
1.	The Complete Reference: Information Security	Mark Rhodes-Ousley	McGraw-Hill	Second	2013
2.	Essential Cybersecurity Science	Josiah Dykstra	O'Reilly	Fifth	2017
3.	Principles of Computer Security: CompTIA Security+ and Beyond	Wm.Arthur Conklin, Greg White	McGraw Hill	Second	2010

Course Outcome:

After completing the course, the learner will be able to:

CO1: Understanding the importance of information protection.

CO2: Comprehending the evolution of information security.

CO3: Utilize established methodologies for implementing and managing security

CO4: Analysing Intrusion Detection and Prevention Systems, Voice over IP(VoIP) and PBX security

CO5: Understanding the security considerations for virtual machines and security aspects of cloud computing

Information Security Practical

B. Sc. (Information Technology)		**Semester – VI**	
Course Name: Information Security Practical		**Course Code: USIT6P2**	
Periods per week (1 Period is 50 minutes)		**3**	
Credits		**2**	
		Hours	**Marks**
Evaluation System	**Practical Examination**	**2½**	**50**
	Internal	**--**	**--**

List of Practical	
1.	**Configure Routers:**
a.	OSPF MD5 authentication.
b.	NTP.
c.	to log messages to the syslog server.
2.	Configure AAA Authentication
a.	Configure a local user account on Router and configure authenticate on the console and vty lines using local AAA
b.	Verify local AAA authentication from the Router console and the PC-A client
3.	**Configuring Extended ACLs**
a.	Configure, Apply and Verify an Extended Numbered ACL
4.	**Configure IP ACLs to Mitigate Attacks and IPV6 ACLs**
a.	Verify connectivity among devices before firewall configuration.
b.	Use ACLs to ensure remote access to the routers is available only from management station PC-C.
c.	Configure ACLs on to mitigate attacks.
d**.**	Configuring IPv6 ACLs
5.	**Configuring a Zone-Based Policy Firewall**
6.	**Configure IOS Intrusion Prevention System (IPS) Using the CLI**
a.	Enable IOS IPS.
b.	Modify an IPS signature.
7.	**Layer 2 Security**
a.	Assign the Central switch as the root bridge.
b.	Secure spanning-tree parameters to prevent STP manipulation attacks.
c.	Enable port security to prevent CAM table overflow attacks.
8.	**Layer 2 VLAN Security**

9.	**Configure and Verify a Site-to-Site IPsec VPN Using CLI**
10.	**Configuring ASA Basic Settings and Firewall Using CLI**
a.	Configure basic ASA settings and interface security levels using CLI
b.	Configure routing, address translation, and inspection policy using CLI
c.	Configure DHCP, AAA, and SSH
d.	Configure a DMZ, Static NAT, and ACLs

Books and References:

Sr. No.	**Title**	**Author/s**	**Publisher**	**Edition**	**Year**
1	Essential Cybersecurity Science	Josiah Dykstra	O'Reilly	Fifth	2017
2	Principles of Computer Security: CompTIA Security+ and Beyond	Wm.Arthur Conklin, Greg White	McGraw Hill	Second	2010
3	The Complete Reference: Information Security	Mark Rhodes-Ousley	McGraw-Hill	2nd	2013