Syllabus

Cyber Security and Social Media Analyst

S No.	NOS/Module Name	Topics	Duration (Hours)		Learning Outcomes
			Theory	Lab	
1	Operating System Basics	• Introduction to different types OS, their Installations, Booting process • Learn to use basic command for Linux and windows OS. • Learn to configure basic services Web, DHCP, DNS, Telnet, SSH TFTP	14	16	• Familiarization with the installation process of windows and Linux OS. • Various types of Installations for Linux • Use of Operating System. • How the OS boots and interacts with underlying Hardware • Practice to use various commands on Linux systems. • File related activity, creation, delete, copy, transfer etc. • Learn to understand the role of services in modern systems. • Configure various services so that end users can use those services.
2	Computer Network	• Network basics: Ethernet Fundamentals and Cabling, ISO-OSI Reference Model, TCP/IP Model, Introduction to LAN, MAN, PAN, WAN, WLAN • IP address, Classes, Classless, CIDR, Prefix, FLSM VLSM, IPv6 addressing	50	70	• Learn about network, type of topologies, LAN, WAN Various models TCP/IP and OSI, layers functions, protocols and their role • Try to create a small network. • IP addressing for Ipv4 and IPv6 • Assign IP Addresses to LAN devices, Network devices, its classes, subnetting topics VLSM and FLSM, assign IPv6 address to various devices including end hosts and network devices • Configure network devices on command prompt using network device operating system. • Learn to enable telnet and ssh access methods on network devices • Configure neighbour discovery protocol CDP and LLDP to create and

		• Network Device OS CLI command, Booting process of router, Router and switch Hardware, enable telnet and SSH access on Router , CDP, LLDP • Basics of routing and switching, routing classification, Static Routing, Default routing, Dynamic routing RIP, RIP Version2 • Types of Switches, installation, configuration, MAC binding, port security on cisco switch, Layer2 security problems and solutions. • Advanced routing protocols EIGRP, OSPF, EIGRP for IPv6 and OSPFv3, theory and configuration and troubleshooting.			understand network scenario. • Configure, verify for static, default routing, RIP, RIPv2 and RIP V3 for IPv6 Networks. • Check router's reading entries in routing table. • Routing table lookup process and next hop selection. • Types of switch, configure Layer2 switches as per requirement. • Types of threats in the network, to mitigate the threats implement layer2 in the switched network. • Assign IP address to layer2 switch as device. • Configure advanced routing protocols like EIGRP, OSPF, and EIGRP for IPv6. OSPFv3. • To verify and troubleshoot the routing protocol for proper functioning. • Configure the access-list to control the traffic passing through the network device and control it using ACLs. • Types of ACLs their configuration and verification. • Control web, Telnet, ssh and FTP traffic using extended ACL • Configure various types of NAT on router. • Check for Internet access after configuring NAT. • Check Nat table. • Troubleshoot NAT, if not working. • Configure FHRP protocol HSRP on router. • Configure VRRP protocol on router • Configure GLBP on router • Configure tracking, change priority • Configure VLAN, Trunk port and access port negotiation protocol DTP, • Configure trunk port and access port. • Configure VLAN trunking protocol IEEE802.1Q on trunk port. • Analyze running spanning tree protocol (STP) on all switches in topology.

		• Access control Lists, standard ACL, Extended ACL, Named ACL • NAT Concept, RFC1918 Addresses, static NAT, Dynamic NAT, PAT configuration and trouble shooting • Gateway load balancing protocols HSRP, GLBP, VRRP • Switching process, LAN VLAN, DTP, VLAN trunking protocol IEEE802.1Q, VTP, STP • WAN protocols HDLC, PPP, frame relay concepts and configuration • Implement port security on cisco switch, Layer2 security problems and solutions.			• Configure WAN connectivity using following WAN protocols. • Configure PPP, HDLC and frame-relay protocol. • Troubleshoot the issues after configuration. • Secure layer2 switch network by implementing port-security. • Troubleshoot and verify the configuration for its functions • Network monitoring software installation. • Configure network devices to SNMP traps to the SNMP manager. • Logging server installation. • Configure network devices as agent to send logs to the logging server. • Ensure security of the data while sending on the Internet. • Implement site-to-site VPN solution on branch and HQ routers. • Verify and troubleshoot the site-to-site router configuration • Configure NTP server on router. • Configure other devices to derive and synchronise time from NTP server.

		• Logging server, SNMP, Bandwidth Management • Virtual Private Networks (VPNs), Concepts, Site-tosite VPN configuration, Easy VPN Server. Concept. • NTP Server, time synchronization on network configuration			

3	Cyber Security	• Information Security: why Information security needed, setup information security in network. • Setting up DB Server, Setting up Proxy server • Linux based Firewall, IPtables, ACLs, etc • Cryptography (Symmetric, Asymmetric) • Information gathering, sniffing, scanning • ARP Cache Poisoning and MITM Attack, IP spoofing, MAC spoofing • DOS & DDOS attack • Accessing remote machine, Privilege Escalation	36	54	• Basic concept Information security. • Techniques to deal with Information Security • Database server installation, working with SQL commands on database, Basic SQL commands. • Setup a proxy server using Linux machine and provide Internet access to other users. • Understand the role of firewall and their needs. • Configure firewall to allow services through the firewall. • Configure ACL for proxy server to deny certain traffic. • Cryptography, encryption concepts. • Popular open crypto algorithms in the Industries. • Best practices and use cases • How hackers collect the information to gain access and how to protect the information • What are the different techniques of attacks and how to defend from these attacks • What is DOS & DDOS attacks and how to defend from these attacks • How hackers gain the access of machines and how to protect from it.

4	Cyber Forensics	• Cyber Law & Digital Forensics • Mobile Forensics	20	10	• Indian Cyber Law • Basics of Live Forensics • Basics of Network Forensics • Basics of Internet Forensics • Basics of Disk Forensics • Basics of Memory Forensics • Basics of Multimedia Forensics • Basic idea about potential evidence • Introduction to Mobile Forensics tools used for acquisitions and analysis of evidence
5	Perception Management	• Social media Analysis and Perception Management • Social Media Publications • Social media Analysis and Perception Management • Gathering Social Media data • Social Media Metrics • Analysing Social Media Data • Social Media Monitoring and Reporting • Sentiment Analysis • Social Network Analysis • Challenges in Social Media Analytics • Content Development and Social Media • Psychological Warfare	50	70	• What is perceptual process • What are the perceptual errors • Introduction to Perception Management and its applications in different sectors • Introduction to snippets • WordPress basics • Customization of snippets using WordPress • Web Development & Website Optimization • Social Media Analytics Basics • Basics of Social Media Conversation • Functional building Block • Introduction to the social Media Data gathering tools • What are the social media metrics used in social media platforms • Understanding Various Aspects of Social Media Analytics • Processes and techniques of Analysing Social Media Data • What is Social Media Listening • Introduction to Social Media Monitoring Tools • Evaluating Social Media • Identifying Opinions

6	Artificial Intelligence/Mac -hine Learning and Disruptive Technologies		10	20	• AI/Ml using python Social Media & AI • Windows Server Administration • Linux Server Administration (including OS security features) • Introduction to Disruptive Technologies (Big Data & Cloud Computing)
Sub Total = 420 hours			180	240	
7	Employability Skills		60		Students will be able to get the additional skills apart from the technical skills, to be job ready
8	OJT/Project		60		Students will be able to learn the working in a job.
Total Duration			**540**		

List of Tools and Equipment

S. No.	Tool / Equipment Name	Specification	Quantity for specified Batch size
1	Classroom	1 (30 Sq.m)	30
2	Student Chair	30	30
3	Student Table	30	30
4	Computer	Intel/AMD multi-core processor (Latest recommended), 16GB RAM, NIC, 1TB SSD/HDD	v
5	Licensed Software	OS (except Open source Linux version, Any reputed Antivirus Software	Per Machine
6	CISCO Router	ISR 2900 series with valid smart net contract	03 Nos.
7	WAN Interface Cards & Cables	HWIC-2T WAN Interface cards, DTE V.35 cable, DCE V.35 Cable, Console Cables	03 Nos. each
8	CISCO Switches	Catalyst 2960, 24 ports	03 Nos.
9	Latest Wireless Router	-	03 Nos.
10	Packet Tracer software OR GNS3 software	-	20 to 40 Nos.
11	Internet connection	50 to 100 Mbps	-
12	Content creation softwares	Adobe Photoshop, Adobe Illustrator, Adobe InDesign, Corel Draw	Per Machine License
13	Any Open source Windows/Linux based media forensic tools like SIFT, Sleuth Kit Autopsy, Oxygen forensic suite, DEFT Zero OR any		Per Machine
14	Kali Linux, Parrot, Metaspoitable framework, CentOS, VirtualBox, VMWare (Open Source/Licensed as applicable)		Per Machine