Course Description ISCP

Topic	Sub-Topic	Sub-Sub-Topic	Tools Used	Expected Course Duration (Hrs)
Introduction to Cyber Security				2
	What is Cyber Security? Statistics and Inferences			
	Need of Cyber Security			
	Common Terminologies			
	Career and Growth			
		Hacking as a Career		
		Domains of Cyber Security		
		Job Opportunities		
	Threats to the Cyber World			
		Non-IT Threats		
		IT Threats		
	Hacking Phases			
		Reconnaissence	Search Engines	
		Scanning		
		Gaining Access		
		Maintaining Access		
		Clearing Tracks		
Basics of Networking				4
	Introduction	Computer Networking Overview		
	How computer Network Works	OSI Model		
		TCP-IP Model		
	Networking Components	NIC Card		
		RJ-45 Card		
		Types of Networks		
		Communication Medium		
		Cables		
	Naming, Addressing & Forwarding			
		MAC Address		
		IP Address		
		Subnet Mask		
		Gateway		
		Classification of IP Addresses		
		Network Address Translation		
		Domain Name Server		
	Subnetting			
	Networking Devices	Hubs		
		Bridges		
		Switches		
		Routers		

		Firewalls		
		WAPs		
	Application Layer	DHCP, FTP/SFTP		
		HTTP/HTTPS, IMAP, LDAP		
		POP, SMTP, SNMP, SSH		
		Telnet, TLS/SSL		
	Transport Layer	TCP/ UDP, RSVP		
	Internet Layer	ICMP, IP		
	Link Layer	MAC, PPP, DSL, ISDN		
	Other Protocols	Finger, MIME / SMIME		
		RTP, TOR, Whois, X.500		
Cryptography				3
	Introduction and Definition of terms			
		Encryption		
		Hashing		
		Encoding		
		Obfuscation		
	Objectives of Cryptography			
		Confidentiality		
		Integrity		
		Authenticity		
		Non-repudiation		
		Accountability		
	Types of Attacks			
		Passive Attacks		
		Active Attacks		
	Introduction to Cryptosystems			
	Encryption			
		Terminologies		
		Model of Encryption		
		Conventions		
	Modern Ciphers			
	Cost Benefit Approach			
	Introduction to Symmetric key cryptography			
	Types of Symmetric Key Cryptography			
		DES		
		AES		
	Asymmetric Key Cryptography			
		RSA		
	Public Key Infrastructure			
		Components of PKI		
		Methods of Certfication		

		Applications of PKI		
		Issues with PKI		
	Hashing			
		Introduction		
		Terminologies		
		Hash vs Cryptographic Hash		
		Classification of Hash functions		
		Applications of Hash		
		MD5		
		SHA		
		HMAC		
		Digital Signatures		
	Cryptographic Protocols			
		Introduction		
		Common Protocols: SSL, TLS, PGP		
	Cryptographic Tools			
		Encryption		
		Hashing		
		File Shredders		
		Steganography		
		Miscellaneous Tools		
	Cryptographic Attacks			
		Brute Force Attack		
		Dictionary Attack		
		Rainbow Table Attack		
		Collision Attack		
		Pre-image Attack		
System Hacking				8
	Basics: Function and Process			
	What do OS do?			
	Types of OS			
		Microsoft Windows		
		Password Management in Windows		
	Hacking Closed System			
		File Swap		
		Mimikatz		
	Hacking Open System			
		Command Prompt		
		Mimikatz		

		Cracking Tools	johntheripper, pwdump, samdump2, ophcrack	
		Privilege Escalation		
		Malware Based		
	Linux Hacking			
		Linux Environment		
		Hacking Closed Linux System		
		Hacking Open System		
	Mac OS X Hacking			
		Password Management		
		Mac OS X File Structure		
		Mac Hacking		
		User Centered Attacks		
Malwares				
	Statistics of Malware Infection			
	Classification of Malwares			
		Virus		
		Worm		
		Bot		
		Trojans		
		Ransomware		
		Rootkit		
		Adware		
		PUP/PUA		
		Keyloggers		
		Browser Hijackers		
	Malware Economy	Impact of Malware Infections		
	Countermeasures			
		Antivirus		
		AdBlockers		
		Firewalls, IDS, IPS		
		Anti-ransomware		
		Strict Usage Policies		
		BYOD Policies		
		User Awareness		
		PC Health monitoring		
		Browser Plugins		
		Online Malware Detection Tools		
Footprinting				3
	Introduction			
	Need of Footprinting			
	Targets of Footprinting			

		IT Infrastructure		
		Organizational Infrastructure		
	Footprinting Techniques			
		Footprinting using search engine		
		Footprinting using Google	Google.com	
		Footprinting using Shodan	shodan.io	
		Footprinting Using WHOIS	whois.com	
		Footprinting Using DNS Queries		
		Footprinting through Social Engineering		
		Footprinting through command-line utilities		
		Footprinting using Tools		
		Footprinting using Source Code Examination		
		Footprinting individuals		
Scanning (Probing)				6
	Introduction			
	Types of scanning			
	Objectives of scanning techniques			
		Scanning for Live Single Systems	ping	
		Scanning for Live Multiple Systems		
		Scanning for Open Ports	Zenmap/Nmap	
	Port Scanning Techniques			
		TCP Connect / Open Scan,Half Open Scan,	Zenmap/Nmap	
		Strobe Scan ,FIN | Null | Xmas Tree Scan,	Zenmap/Nmap	
		FTP Bounce Scan ,UDP Scan	Zenmap/Nmap	
	Port scanner tools			
		Hping, NetScan Tool,		
		Strobe (Super optimised TCP port surveyor)		
		Scanning for System Information		
	Vulnerability Scanning		Nessus, OpenVas	
		Vulnerability Scanner Tools		
	Determining Network Architecture,		Nessus	
		Tools for mapping Network Architecture	LanState Pro, Network Mapper	
	Conclusion			
Web Server Security				8
	Web Server			
		File Servers		
		Application Servers		
		Message Servers		
		Proxy Servers		
		Database Servers		

		Mail Servers		
	Web Server Architecture			
		Concurrent Approach		
		Single Process Event driven approach		
	Attacking Methodology			
		Web Server Attack Vectors		
		Footprinting		
		Scanning		
	Gaining Access			
		Web Server Attacks	metasploit	
	Privilege Escalation			
		Vertical Privilege Escalation		
		Horizontal Privilege Escalation		
		Remote Code Execution		
		DoS		
		Memory Corruption		
		Metasploit		
	Impact of WebServer Attacks			
	Countermeasures to Web Server Attacks			
Firewalls, IDS and IPS				2
	Types of firewall			
		Packet-filtering firewalls		
		Stateful inspection firewalls		
		Proxy firewalls		
		Circuit-level gateways		
		Application-level gateways		
		Stateful Multilayer inspection firewalls		
	Firewall Requirement Analysis and Implementation			
		Requirement analysis		
		Practical implementation of Firewall		
	Unified Threat Management			
		Advantages of using UTM		
		Challenges of using UTM		
	Evading Firewalls			
	Firewall Identification			
		Port Scanning		
		Firewalking		
		Banner Grabbing		
	IP Address Spoofing			
		Source Routing		

		Tiny Fragments		
		Bypass Blocked Sites Using IP Address in Place of URL		
		Bypass Blocked Sites Using Anonymous Website Surfing Sites		
		Bypass a Firewall Using Proxy Server		
		Bypassing Firewall through ICMP Tunneling Method		
		Bypassing Firewall through ACK Tunneling Method		
		Bypassing Firewall through HTTP Tunneling Method		
		Bypassing Firewall through SSH Tunneling Method		
		Bypassing Firewall through External Systems		
		Bypassing Firewall through MITM Attack		
		Bypassing Firewall through Content		
	Intrusion Detection System (IDS)			
		What is IDS?		
		How does IDS work ?		
		Functions of IDS		
	Classifications			
		Analyzed activity		
		Detection method		
	IDS Evasion Tools			
	Firewall Evasion Tools			
		Traffic IQ Professional		
		TCP over DNS		
		Packet Fragment Generator		
	Intrusion Prevention System (IPS)			
		How does IPS work?		
		What is the function of IPS?		
	Classification			
		Host-based intrusion prevention system (HIPS)		
		Network behavior analysis (NBA)		
		Wireless intrusion prevention systems (WIPS)		
	Detection methods			
		Signature-Based Detection		
		Statistical anomaly-based detection		
		Stateful Protocol Analysis Detection		
		Limitations		
	Free and open source systems			
	Evading IDS			
	Honeypot			
		Types of honeypot		

		How does it work?		
		How to setup honeypots?		
Web Application Security				10
	Basics of Web Application			
		Architecture of Web Applications		
		Need and use of Web Applications		
	Pasive Information Gathering		Maltego, webapplyzer	
		Google Hacking	GHDB	
		Whois Lookup	netcraft, whois.net	
		DNS Interrogation	mxtoolbox, dns queries, virustotal	
	Active Information Gathering			
		1.Port Scanning		
		2.Service Scanning		
		3.OS Fingerprinting		
		4.Enumerating Web Application framework		
		5.Web App. Content Discovery	Burpsuite, HTTrack, BlackWidow	
	Check Authentication Mechanism			
		Username		
		Passwords		
		Session		
	Vulnerabilities in Authorization Mechanism			
		Directory Traversal (horizontal and vertical directory)		
		Bypassing Authorisation Schema		
		Privilege Escalation		
		Insecure Direct Object reference		
	Injection Attacks			
		Web Script Injection		
		SMTP Injection		
		SQL Injection		
		LDAP Injection		
		XPath Injection		
		Command Injection Attack		
	Web Application Vulnerabilities and its Defences		Burpsuite, OWASP ZAP	
		Insufficient Transport Layer Protection		
		Security Misconfiguration		
		Insecure Cyptographic Storage		
		Buffer Overflow		
		Cross Site Request Forgery attack		

		(CSRF)		
		Cross Site Scripting (XSS)		
		Redirection Attack		
		Improper Error Handling		
		Information Leakage		
		Failure to Restrict URL Access		
		Security Management Exploits		
		Malicious File Execution		
		Captcha Attacks		
		Authentication Hijacking		
		Network Access Attacks		
		Cookie Snooping		
	Web Application Security Scanner			
		Commercial Tools	Acunetix, Nessus, BurpSuite, OWASP ZAP	
		Software-as-a-Service Providers		
		Free / Open Source Tools		
		List of Tools		
Injection				10
	SQL Injection		Sqlmap, Sqlninja	
		Types of SQL injection		
		SQL Injection tools		
		HTTP GET and POST request protocols		
		Basic queries of SQL injection		
	Code Injection			
		Types of Code Injection		
		Vulnerability of Code Injection		
		Prevention of Code Injection		
	File Inclusion Vulnerability			
		Types of File Inclusion		
	Command Injection			
		How to perform command injection?		
	How to prevent SQL Injection			
Social Engineering				2
	Statistics			
	Stages of Social Engineering Attack			
		Information Gathering		
		Developing Relationship		
		Exploitation		

		Execution		
		Target Profiling		
	Types of Social Engineering Attack			
		Digital Attacks	SET Toolkit	
		Personal Attacks		
		Impersonation Attacks		
		Techno-Personal Attacks		
	Mitigation Strategies			
		Training of Stakeholders		
		Policy Implementation		
Spoofing				3
	Objectives of Spoofing			
	Types of Spoofing			
		IP Address Spoofing	Ultrasurf, free-proxy-lists.net, vpnbook.com/webproxy, protonvpn	
		MAC Address Spoofing	Technitium MAC Changer (Windows), Macchanger (linux)	
		Call Spoofing	crazycall.net, spooftel.com, spoofcard.com	
		SMS Spoofing	spooftel.com, spoofcard.com	
		URL Spoofing		
		Email Spoofing	Emkei.cz, PHP Mailer	
		ARP Spoofing		
		DNS Spoofing		
	Legitimate use and Impact of spoofing			
Mobile Application Security				6
	Mobile Application Security			
	Need for Mobile Application Secuity Testing			
	Android Architecture			
		Application framework		
	Interaction with Android Devices			
		Android Emulators and Devices		
		Android Debug Bridge (ADB)		
		Downloading and installing applications with ADB		
	Android Network Analysis			
		Setting Up a Proxy For Android Emulator		
		Setting Up a Proxy For Android Device		
		Data Capturing(MITM Attack)		
		Download And Install CA Certificate		
		SSL Data Capturing(MITM Attack)		
	Android Application Pen-Testing			

		Android APK Reverse Engineering		
		Static Manual Testing with Drozer		
		Automation testing with MobSF		
		OWASP top 10 Mobile Vulnerabilities		
	Rooting of Android Devices			
		Preparing a Device for Rooting		
		Tools used for Rooting		
		Unrooting Android Device		
Denial of Service Attacks				2
	DDoS attacks			
	Statistics related to DoS			
	Types of DDoS attacks			
		Smurf Attack		
		DNS Flood Attack		
		DNS Amplification Attack		
		Ping of Death		
		ICMP Flood		
		NUKE Attacks		
		NTP Amplification		
		UDP Flood		
		SYN Attacks		
		Reflected DoS		
		Teardrop		
		Peer to Peer		
		Slowloris		
		RUDY Attack		
		XML Attack		
		HTTP Flood		
		SNMP attack		
		Other Types		
	Sources & tools of DDoS			
		LOIC		
		XOIC		
		HOIC		
		Botnets		
		Insecure IoT Devices		
		JMeter		
		Dirt Jumper		
		OWASP HTTP DOS Tool		
	Detection of DoS Attacks			
	Mitigation Strategies			
		Firewalls		

		Redundant Resources		
		Third Party Service providers		
		Preventing Flooding attacks		
	Unintentional DoS			
	Economics of DoS			
	Impact of DoS Attacks			
	Buffer Overflow Attack			
		Stacks		
		Heaps		
		Shellcodes		
	Memory Segment Overflow			
		Memory Organisation		
		Stack Overflow		
		Heap Overflow		
		Impact		
Cloud Security				2
	What is Cloud Security?			
	Deployment models of Cloud			
		Private		
		Public		
		Hybrid		
		Virtual Private Cloud		
		Community Cloud		
	Categories of Cloud Services			
		1. IaaS (Infrastructure as a Service)		
		2. PaaS(Platform as a Service)		
		3. SaaS(Software as a Service)		
		4. DaaS (Desktop as a Service)		
		5. Communications as a Service (CaaS)		
		6. Network as a Service (NaaS)		
	Cloud Benefits			
	Information Management and Data Security			
		Information Management		
		Data Security		
		Volume storage		
		Object storage		
		Logical vs physical locations of data		
		Data Loss Prevention		
		Detecting Data Migration to the Cloud		

		Database Activity Monitoring and File Activity Monitoring		
		Encryption in IaaS, PaaS & SaaS		
		Data Backup		
		Data Dispersion		
		Data Fragmentation		
	Portability and Interoperability			
		Portability		
		Interoperability		
		SAML and WS-Security		
		Lock-In considerations by IaaS, PaaS & SaaS delivery models		
		Mitigating Hardware Compatibility Issues		
	Cloud Security Model	Jerico Cube Model		
	Cloud Security			
		Cloud Security Control Layers		
		Responsibility of Cloud Security		
		NIST Recommendations for Cloud Security		
		Cloud Computing Security Considerations		
		Placement of Security Controls in the Cloud		
		NIST		
		Cloud Security Tools		
		Cloud Encryption Tools		
		Cloud Service Providers		
	Privacy and Security Concerns			
	Limitations of Cloud			
Wifi Hacking				8
	Wi-Fi Security			
		Types of Wireless Networks		
		Benefits of Wireless Technology		
		Disadvantages of Wireless Technology		
		Introduction to 802.11WLAN Protocols		
	Basic concepts	Network Basics		
	Wireless Attack Scenarios			
		MAC Spoofing		
		Packet Injection		
		Packet Sniffing		
		Pawning Beacon Frames (Fake Access Points)		
		De-auth Attack		
	Bypassing WLAN Authentication			
		Hidden SSIDs		

		Unmasking hidden SSIDs		
		What is MAC Filter?		
		Grabbing MAC Address of Associated Clients (MAC Filter)		
	Cracking WEP Wi-Fi networks			
		Logic behind WEP Wi-Fi encryption		
		Vulnerabilities in WEP		
		Cracking WEP		
		Speed-Up WEP Cracking		
		Countermeasures to avoid WEP cracking		
	Cracking WPA/WPA2 Wi-Fi networks			
		WPA (Wi-Fi Protected Access) Wi-Fi Network		
		WPA2 (Wi-Fi Protected Access 2) Wi-Fi Encryption		
		WPS (Wi-Fi Protected Setup)		
		Vulnerabilities in WPS		
		Countermeasures for WPS vulnerabilities		
		Vulnerabilities in WPA/WPA2		
	Cracking WPA/WPA2			
		Types of WPA/WPA2 Cracking	aircrack-ng, airmon-ng, airodump-ng	
		How to Crack WPA/WPA2		
		Speed WPA Cracking		
	Client Side Wi-Fi Attacks			
		Cracking WEP		
		Requirements fo Conducting Cracking at Client Side		
		Cracking WPA/WPA2		
	Man in the Middle Attack			
		Executing MITM Attacks		
		Types of MITM Attacks		
	Wireless Penetration Testing Methodology			
		Pentest		
		Penetration Testing Tool		
		Phases of Penetration Testing Methodology		
IoT Security				2
	Technical Overview			
	Elements of IoT infrastructures			
		IOT Network Architecture and Design		
		IOT and the 3 C's		
		Hardware		

		Firmware		
		Communication Channels		
	IoT Attack Surfaces			
	Common Vulnerabilities in IoT Devices			
	Securing IoT			
		1. Cryptographic Solutions		
		2. Security Features of IoT protocols		
		3. Security Management		
	Advantages of IoT			
	Challenges in IoT			
Cyber Laws and Compliances				2
	Cyber Crimes	Crimes against People, Property, Government and society		
	Statistics of Cyber Crime	India and World		
	Cyber Laws			
		Penalties, Compensation and Adjudication sections		
		Offenses sections		
	Case Studies	Cyber cases listed in IT Act 2000		
	Recent Cyber Crimes around the world			
		Cyber Crime against Finances		
		Cyber Crime against Individuals and Organizations		
		Ransomware in Hospitals		
		Credit Card Frauds		
		Cyber Terrorism		
	How to Report Cyber Crimes			
	Recent Initiatives in India			
	Security Compliances			
		Types of Compliances		
		ISO 27001		
		ISO 27002		
		PCI DSS		
		COBIT 5		
		NCIIPC		
Pentesting				4
	Penetration testing			
	Vulnerability Assesment vs Penetration testing			
	Importance of Penetration testing			
	Advantages of Pentesting			
	Methods of Pentesting			
		Black Box testing		
		White Box testing		
		Grey Box testing		

		Bug Bounty		
	Penetration Testing Execution Standard			
		OWASP Testing Guide		
		NIST SP800-115		
		New PCI DSS Guidance		
		FedRAMP		
		PTES		
	Legal Authority			
		Scope of Work		
		Damage Control		
		Indemnification		
		Hack-Back		
		Professionalism		
		Licensing and Certification		
		Privacy Issues		
		Data Ownership		
		Duty to Warn		
	Stages of Pentesting			
		1.Footprinting		
		2. Scanning		
		3. Enumeration		
		4. Performing Penetration Tests		
		Web Application Pentesting		
		OWASP Top 10 for Mobile		
		Servers		
		Network Penetration Testing		
	Reporting			
		Structure of a Report		