PG Diploma in IT Infrastructure & Systems Security

Fundamental of Computer Networks - 80 Hours

Introduction to communication system, Overview of Transmission Media, OSI Layers, TCP/IP Models, Router IOS & Security Device Manager, Managing an Internetworking Router, Overview of LAN (local area networks), VLAN (virtual local area network), Configuration of switch, Overview of STP, Discussion of Networking Protocols, IP Addressing (Fixed Length Subnet Masking, Variable Length Subnet Masking, Classless Inter Domain Routing), Static Routing and Dynamic Routing (RIP, IGRP, EIGRP, OSPF), Introduction to NAT, Introduction to IPv6, Introduction of WAN, Infrastructure Security, Software defined network

Concepts of Operating System and Administration - 180 Hours

Windows Operating System and Security Issue (80 Hrs)

Overview of windows operating system, Installation of windows operating system, Windows 11/ server 2022 or above, , Overview of Administrative Tasks and Tools, Windows Server Backup (WSB), Network Configuring, Implementation of infrastructure of windows networks, Active Directory Domain Services (ADDS), DNS, DHCP and IPAM, Local Policies, Group Policies, Configuration of IIS web server, Deploying Windows with WDS, Hyper-V & Storage Solutions, File Server Resource Manager (FSRM), Network Policy Server (NPS),Network Load Balancing (NLB), Exchange server, Maintenance and troubleshooting, Power shell Scripting, Windows Administration using power shell, Background Jobs and Remote Administration.

Linux Operating System and Security Issue (100 Hrs)

Systems Concepts, Startup Files, Linux boot process, Installation of Linux(Ubuntu 22 or above / server cent OS 8 / Debian 12), Basic linux commands, Configuring the GRUB boot loader, Disk partition, Controlling and managing Services, Repository configuration, User administration of Linux, Network Configuring, Network Teaming/Load balancing, Define network route, Using SSH for network communications, Using VNC for remote management, Network Authentication, Patches & updates, System Configuration Files, Perform System Management, X configuration server, Package management, The Samba Server, Configuring a DHCP server, Configuring a DNS server, Configuring the Apache web

server, Maintenance and troubleshooting, SE LINUX/ APParmor, Basic Service Security, Log Management and NTP, BIND and DNS Security, Network Authentication: RPC, NIS and Kerberos, Apache security(SSL), Bash Scripting, Introduction to BASH Command Line Interface (CLI) Error Handling Debugging & Redirection of scripts, Control Structure, Loop, Variable & String Conditional Statement, Regular Expressions, Automate Task Using Bash Script, Security patches, Logging & Monitoring using script.

Programming Concepts - 70 Hours

i.MYSQL (20 Hrs)

Introduction to MYSQL, Installing and Configuring MYSQL, Creating and Dropping Database, Queries in MYSQL

ii. Python (50 Hrs)

Introduction to Python, Python basics, Data Types and variables Operators, Looping & Control Structure List, Modules Dictionaries, string Regular Expressions, Functions and Functional Programming, Object Oriented Linux Scripting Environment, Classes, Objects and OOPS concepts, File and Directory Access Permissions, Libraries and Functionality Programming, Servers and Clients Web Servers and Client scripting, Exploit Development techniques. Writing plugins in Python, Exploit analysis Automation Process, Debugging basics, Task Automation with Python

Security Concepts - 110 Hours

Web Application Security (24 Hrs)

OWASP Top 10 –2021, Injection and Inclusion, Cross Site Scripting, Injection in stored procedures, Denial of Service, Buffer Overflows and Input Validation, Access Control,

DevOps Security, API Security, OWASP top 10 Cloud security Risks, Secure Code Review, SAST and DAST tools, Case Study on Web Application Framework, use browser guard Firefox add-on also to detect Malicious and Suspicious Webpages. Web Application Security Risks, Identifying the Application Security Risks, Threat Risk Modelling, Other HTTP fields, Data Extraction, Advanced Identification/Exploitation

Mobile Security (20 Hrs)

Introduction to Android Architecture, Android File Structure, Android Build Process, Android App fundamentals, Android Security Model, Device Rooting, Android Debug bridge, Penetration Testing Tools, OWASP Top 10 Mobile App vulnerabilities, Attacks on Android Apps, Web based attacks on Android devices, Networks based attacks, Social Engineering attacks, Overview of Mobile Malware, Android App Analysis

Ethical Hacking (66 Hrs)

Introduction to Ethical Hacking, Identifying Different Types of Hacking Technologies, Understanding the Different Phase Involved in Ethical Hacking, Types of Hacker Classes, Goals of Attackers, Functionality and Ease of Use Triangle, Ethical Hacking procedure, Creating a Security Evaluation Plan, Foot-printing and Social Engineering, Tracerouting, Network Scanning and Vulnerability Scanning, SYN, Stealth, XMAS, NULL, IDLE and FIN Scans, TCP Communication Flag Types, Banner Grabbing and OS Finger printing Techniques, Using Proxy servers in launching an Attack, Http tunneling Techniques, IP Spoofing Techniques, Enumeration, Password-cracking Techniques, Redirecting the SMB Logon to the attackers, SMB Redirection, SMB Relay MITM Attacks and Countermeasures, NetBIOS DOS Attacks, DDos Attack, Password-Cracking Countermeasures, Active/Passive online Attacks, Offline Attacks, Keyloggers and other Spyware Technologies, Trojans and Backdoors, Overt and Covert Channels, Reverse-connecting Trojans, Netcat Trojan, Indications of a Trojan Attacks, Wrapping, Trojan Construction Kit and Trojan Makers, The countermeasure Techniques in Preventing Trojans, Trojan Evading techniques, System File Verification, Virus and a Worm, Antivirus Evasion Techniques, Virus Detection Methods, Protocols Susceptible to Sniffing, Active and Passive Sniffing, ARP Poisoning, Ethereal Capture and Display Filters, MAC Flooding, DNS Hacking, DNS Spoofing Techniques, Sniffing Countermeasures, Types of DOS Attacks, Smurf Attacks, SYN Flooding, Spoofing vs Hijacking, Types of Session Hijacking, Steps to perform session Hijacking, Prevention of session Hijacking, Hacking Web Servers, Web Application

Vulnerabilities, Web- Based Password Cracking Techniques, Wireless Hacking, WEP, WPA Authentication Mechanisms and Cracking Techniques, Wireless Sniffers and Locating SSIDS, Wireless hacking Techniques, Methods used to secure Wireless Networks, IDSs, Honeypots and Firewalls.

Compliance Audit - 30 Hours

Cybersecurity Challenges in Organizations, Compliance and Regulations for Cybersecurity ,Compliance Basics, Compliance Frameworks and Industry Standards, National Institute of Standards and Technology (NIST) , General Data Protection Regulation (GDPR), International Organization for Standardization (ISO) 2700x, SOC Reports, SOC Reports - Auditor Process Overview, Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS),COBIT Framework, Center for Internet Security (CIS) Critical Security Controls, ITAA 2008, Digital Personal Data Protection Act 2023

Network Defense and Countermeasures (NDC) - 70 Hours

Security Fundamentals, Firewalls, Types of Firewalls, Linux firewall IP tables, Overview of NextGen Firewall, Limitations of firewall, Intrusion Detection and Prevention, Intrusion risks, Security policy, Monitoring and reporting of traffics, Traffic shaping, Investigating and verifying detected intrusions, recovering from, reporting and documenting intrusions, Define the Types of intrusion Prevention Systems, Intrusion prevention system basics, Limitations of Intrusion Prevention System, Spoofing Detection & Prevention, Dos & Dos mitigation techniques, Qos Policy, Introduction of Web Application Firewall, Packet Signature and Analysis, Virtual Private Networks, Deploy and managing VPN, VPN Performance tuning and error handling, DMZ and virtual host, Unified Threat Management, Threat Hunting Model, Introduction of Reverse proxy and policies.

Cyber Forensics - 40 Hours

Introduction to Cyber Crime and Cyber Forensics, Basic Forensic Principles, Computer Forensics, Types of Cyber Forensics Techniques, Cyber Forensics Procedures, Detecting

Incidents, Handling Evidence, Encoding and Encryption, Cyber Forensics Tools: Sysinternals Suite, FTK Forensics Tool kit, FTK Imager, OSF, Hex, Cyber check Suite, Live system forensics, Linux Forensics, An introduction to Mobile forensics.

Public Key Infrastructure - 50 Hours

Understand Basic Encryption Concepts, File Encryption, Encryption Folders (Graphical/ using cipher), Cryptographic Fundamentals, Cryptographic Ciphers (Symmetric and Asymmetric), Protocols (History, Usage, Key generation, Ciphering message), Symmetric Key Encryption (DES, AES, RC5), Asymmetric Key Encryption (RSA, ECC), Diffie-Hellman Key Exchange, Attacks against encryption, Cryptographic issues, Secure Hashing Methods, SHA Secure Hash algorithm, HMAC, PKI Fundamentals, Digital Signature, Digital Certificate, CA, Trust Model, Certificate Issuance Process, Certificate Revocation (CRL, OCSP), Types and Classes of Certificate, Introduction to Aadhaar and e-Sign, Time stamping Services, Public Key Cryptography Standards, PKCS, FIPS 140-2, Strong Authentication,
Single Factor and Multi-factor authentication, Single Sign-on Solutions,
Open-ID and OAUTH, Graphical Passwords, Authentication Protocols, FIDO Authentication, Zero Trust Architecture, Securing Websites and Emails, SSL, TLS, PGP and S/MIME.

Introduction to ITIL and Data Center Management (16 Hrs)

Service Strategy, Service Design, Service Transition, Service Operation, Continual Service Improvement, Introduction to DCM, Data Center design, Data Center Security Procedure, Server Security

DevOps (74 Hrs)

Storage area network, Virtualization, Docker, kubernetes, Introduction of Virtual Private Cloud (VPC), Private Cloud Setup, Automation Using Cloud API, Server Orchestration, Cloud Logging and monitoring, Introduction to DevOps, Docker, kubernetes, Dockerswam, Container, CI/CD Pipelines, Version Control system,

containerization with Docker, GitHub, AWS, Micro Service Deployment, Terraform, Ansible.

Getting more from Open day light

- Open Day light and AAA
- Introduction to OVSDB Virtualization
- Application Intents and Group Based Policy
- Service Function Chaining
- LISP Flow Mapping
- Virtual Tenant Networks

Aptitude & Effective Communication - 90 Hours

Aptitude: Percentage, Profit & Loss, Ratio & Proportion, Average, Mixture & Allegation, Simple Interest & Compound Interest, Seating Arrangements (Linear & Circular), Ages, Time, Speed & Distance, Trains, Boats & Streams, Time & Work, Wages (Man days), Pipes & Cisterns, Clocks, Permutations & Combinations, Probability,

Effective Communication: Personality Development, English Grammar, Correct Usage of English, Listening Skills, Reading Skills, Writing Skills, Formal Application Writing, Public Speaking, Presentation Skills, Group Discussions, Personal Interviews

Project - 90 Hours

It will cover various aspects, including project planning, requirements gathering, solution design, implementation, testing, and documentation.