SYLLABUS

UNDER
SKILL DEVELOPMENT CENTRE

CERTIFICATE COURSE

IN

CYBER SECUIRITY

DURATION- 6 MONTHS

Effective from the Academic Session 2021

SIDHO-KANHO-BIRSHA UNIVERSITY
PURULIA, WEST BENGAL

In modern days our daily life becomes digital life or computer life in which internet becomes very essential part. But now-a-days like others, this life is not smooth at all and not free from threats, thefts and crimes. Cyber security is introduced to protect all these systems from the malicious attacks. Our University has introduced a certificate course on Cyber Security of 6 months duration of which

The Objective is to provide skills in cyber security and to make students ready to work in industry. Students will directly get the practical knowledge and live industrial training after which they will get training certificate from the University through examination and can apply for job in various industries as well as higher studies also.

CYBER SECURITY

OBJECTIVE OF THE COURSE

In modern days our daily life becomes digital life or computer life in which internet becomes very essentialpart. But now-a-days like other, this life is not smooth at all and not free from threats, thefts and crimes.
Cyber security is introduced to protect all these systems from the malicious attacks.
Now objective of this course is to provide skills in cyber security and to make students ready to work in industry. Students will directly get the practical knowledge and live industrial training after which they willget training certificate from the University through examination

PROGRAMME OUTCOMES

After completing the course and having the training certificate from University students are eligible for industrial work. As cyber security has high demand in job world due to shortage of cyber security professionals, students have a great opportunity to get job in it. On the other hand, to being able to workfrom home is another benefit as cyber security is a technology-based field.

SCCYST 101: Cyber Security and Cryptography

Introduction to Cyber Security: What is Cyber Security? Need of Cyber Security, CommonTerminologies, Career and Growth, Threats to the Cyber World, Hacking Phases

Cyber Laws and Compliances: Cyber Crimes, Statistics of Cyber Crime, Cyber Laws, Case

Studies, Recent Cyber Crimes around the world, How to Remove Cyber Crimes, Recent Initiatives in India, SecurityCompliances

Basics of Networking: Introduction, How computer Network Works, Networking Components, Naming, Addressing & Forwarding, SubneLing, Networking Devices, Application Layer, Transpofi Layer, InternetLayer, Other Protocols: Finger, MIME / SMIME RTP, TOR, Whois, X.500.

Cryptography: Introduction of Encryption, Hashing, Encoding, Obfuscation etc, Objectives of Cryptography, Passive Attacks Active Attacks, Cryptosystems, Encryption; Modern Ciphers; Cost BenefitApproach; Symmetric key cryptography; Types of Symmetric Key Cryptography; Asymmetric Key Cryptography; Public Key Infrastructure; Hashing; Cryptographic Protocols: SSL, TLS, PGP; Cryptographic Tools; Cryptographic Attacks;

Foot printing: Introduction, Need and targets of Foot printing; Foot printing Techniques;

Network Scanning: Introduction, Types and Objectives of scanning techniques; Pofi Scanning Techniques;Pofi Scanner Tools; Vulnerability Scanning; Determining Network Architecture; Conclusion**.**

SCCYST 102: Cyber Threats and its Preventions

Spoofing: Objectives and Types of Spoofing; Legitimate use and Impact of

spoofing;

System Hacking: Basics: Function and Process; What do OS do? Types of OS; Hacking Closed System;Hacking Open System;

Web Application Hacking: Basics of Web Application; Passive and active Information Gathering; CheckAuthentication Mechanism; Vulnerabilities in Authorization Mechanism; Injection Attacks; Web Application Vulnerabilities and its Defenses; Web Application Security Scanner.

Injection: SQL Injection; Code Injection; File Inclusion Vulnerability; Command Injection; How toprevent SQL Injection

Web Server Hacking: Various Web Server; Web Server Architecture; Attacking Methodology; GainingAccess; Privilege Escalation; Impact of Web Server Attacks; Countermeasures to Web Server Attacks.

Firewall, IDS and IPS: Types o Firewall; Firewall Requirement Analysis and Implementation; Unified Threat Management; Evading Firewalls Firewall Identification; IP Address Spoofing:

tiny fragments, Bypass Blocked Sites, Bypassing Firewall; Intrusion Detection System (IDS) and its classifications; IDS Evasion Tools Firewall Evasion Tools; Intrusion Prevention System (IPS) and its classifications; Detectionmethods; Free and open source systems Evading IDS Honeypot.

Denial-of-Service (DOS): DDoS Attacks; Statistics related to DoS; Types of DDoS Attacks; Sources & tools of DDoS; Detection of DoS Attacks; Mitigation Strategies; Unintentional DoS; Economics of DoS; Impact of DoS Attacks; Buuer Ovefilow Attacks; Memory Segment Ovefilow.

Social Engineering: Statistics; Stages of Social Engineering Attacks; Types of Social Engineering Attacks;Mitigation Strategies;

SCCYST 103: Cyber Security II

Mobile Security: Mobile Application Security; Need for Mobile Application Security Testing; Android Architecture; Interaction with Android Devices; Android Network Analysis; Android Application Pen- Testing; Rooting of Android Devices

Wireless Hacking: Wi-Fi Security; Wireless Attacks Scenarios; Bypassing WLAN Authentication; Cracking WEP Wi-Fi networks; Cracking WPA/WPA2 Wi-Fi networks; Vulnerabilities in WPA/WPA2;Client Side Wi-Fi Attacks; Man in the Middle Attacks; Wireless Penetration Testing Methodology;

Cloud Security: What is Cloud Security? Deployment models of Cloud; Categories of Cloud Services; Cloud Benefits; Information Management and Data Security; Pofiability and Interoperability; Cloud Security Model; 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;

Internet of Things (IoT) Security: Technical Overview; Elements of IoT infrastructures; IoT Attacks Sufiaces; Common Vulnerabilities in IoT Devices; Securing IoT; Advantages of IoT; Challenges in IoT;

Pentesting: Penetration testing ; Vulnerability Assessment vs Penetration testing; Importance of Penetration testing; Advantages of Pentesting; Methods of Pentesting; Penetration Testing ExecutionStandard; Legal Authority; Stages of Pentesting; Repofiing;

Bug Bounty: Recon for Bug Bounty Web; Server Hacking; Identity Management Testing; CMSVulnerability Hacking; WAF Bypass;

SCCYSP 104: Web Application Penetration Test (WAPT)

Vulnerability Assessment of WAPT; Project Management; Professional Exposure

SCCYSP 105: Network Penetration Testing (NPT)

Vulnerability Assessment of NPT; Project Management; Professional Exposure