संगणक शास्त्र प्रशाळा, कवयित्री बहिणाबाई चौधरी उत्तर महाराष्ट्र विद्यापीठातर्फे आयोजित प्रमाणपत्र अभ्यासक्रमात सहभागी होणेबाबत...

कवयित्री बहिणाबाई चौधरी उत्तर महाराष्ट्र विद्यापीठ परिक्षेत्रातील सर्व इच्छुक विद्यार्थी / व्यक्ती यांच्यासाठी फेब्रुवारी व मार्च या कालावधीत कवयित्री बहिणाबाई चौधरी उत्तर महाराष्ट्र विद्यापीठ, संगणक शास्त्र प्रशाळा येथे खालील प्रमाणपत्र अभ्यासक्रमांचे आयोजन करण्यात येणार आहे.

१) Cyber security certificate course: शनिवार, रविवार (चार आठवडे)
अभ्यासक्रमाचा एकूण कालावधी : आठ दिवस (४५ तास) शुल्क: रु. ५००० मात्र

२) Digital Ethical Hacking certificate course:शनिवार, रविवार(चार आठवडे)
अभ्यासक्रमाचा एकूण कालावधी : आठ दिवस (४५ तास) शुल्क: रु.७५०० मात्र

वरील अभ्यासक्रमांचा कालावधी खालीलप्रमाणे:

Sr. No.	Day	Date
1	Saturday	
2	Sunday	
3	Saturday	
4	Sunday	
5	Saturday	
6	Sunday	
7	Saturday	
8	Sunday	

संगणक जगतामध्ये अतिशय आवश्यक असे हे अभ्यासक्रम असून IT Industry साठी लागणारी कौशल्य वृद्धिंगत होण्यासाठी हे अभ्यासक्रम उपयुक्त आहे. या अभ्यासक्रमामुळे आपल्याला विविध क्षेत्रात करिअर संधी उपलब्ध होऊ शकतील.

सर्व अभ्यासक्रमाबद्दल सविस्तर माहिती खाली दिलेली आहे.

विशेष सूचना:

१) पूर्वी नोंदणी केलेल्यांनाही परत नोंदणी करणे आवश्यक आहे.

२) online नोंदणी झाल्यावर कोर्स फीच्या किमान ५०% रक्कम जोपर्यंत संगणक शास्त्र प्रशाळेत रोखीने प्रत्यक्ष जमा होत नाही तोवर नोंदणी नक्की झाली असे समजले जाणार नाही.

३) सर्व अभ्यासक्रमांना मर्यादित जागा असून शुल्कासहित प्रथम नोंदणी करणाऱ्यांना

प्रथम प्राधान्य असेल.

सर्व इच्छुक विद्यार्थी / व्यक्तींनी अधिक माहितीसाठी संपर्क करावा.

संगणक शास्त्र प्रशाळा,
क. ब. चौ. उत्तर महाराष्ट्र विद्यापीठ, जळगाव. (०२५७-२२५७४५३)
प्रा. कविता तु. पाटील (संपर्क क्र. ९९७०९१३७८९) इमेल: meetpatilkavita@gmail.com

सर्व इच्छुक व्यक्तींनी खाली दिलेल्या लिंक वर नाव नोंदणी करावी.
लिंक: : https://forms.gle/LJmhQi3v4XYP6CQ56

सूचना: कोर्स मिश्रित मोडमध्ये घेण्यात येईल (ऑनलाइन तसेच ऑफलाइन)

List of topics - Cyber security certificate course

1) Certificate in Cyber Security-

1. Introduction to Cyber Security, 2. Latest Technological Trends, 3. Basics of Networking, 4. Virtualization and installation of OS on virtual Box, 4. Passwords, 5. Web browser security, 6. Firewall And UTM, 7. Physical Security Closed circuit television cameras (CCTV), 8. Mobile Security, 9. Email Security, 10. Malware, 11. Cryptography, 12. Wireless Security,13. Ethical Hacking, 14. Google Hacking, 15. Virtualization and Cloud Computing, 16. Cloud Computing, 17. Cyber Crime and Cyber Laws, 18. Cyber laws (Information Technology Act 2000 & 2008), 19. ISO 27001, 20. IP based communication: (VOIP), 20. Protection of information Assets, Planning and implementation of BC/DR, 21. Make reports based on test results and make enhancements to existing security solutions, 22. Manage your work to meet requirements, 23. Work effectively with colleagues, 24. Maintain a healthy, safe and secure. 25. working environment.

SR NO	Modules
1	Introduction to Cyber Security
2	Latest Technological Trends
3	Basics of Networking
4	Virtualization and installation of OS on virtual Box.
5	Passwords
6	Web browser security
7	Firewall And UTM
8	Physical Security Closed circuit television cameras (CCTV)
9	Mobile Security
10	Email Security
11	Malware
12	Cryptography
13	Wireless Security
14	Ethical Hacking
15	Google Hacking
16	Virtualization and Cloud Computing
17	Cloud Computing
18	Cyber Crime and Cyber Laws
19	Cyber laws (Information Technology Act 2000 & 2008)
20	ISO 27001
21	IP based communication: (VOIP)
22	Protection of information Assets, Planning and implementation of BC/DR
23	Make reports based on test results and make enhancements to existing security solutions
24	Manage your work to meet requirements
25	Work effectively with colleagues
26	Maintain a healthy, safe and secure working environment

Cyber Security Course Curriculum

Module 1

Introduction to Cyber Security

1. What is cyber security?
2. Need for cyber security (case studies)
3. statistics
4. Layered approach to cyber security

Objective

- The objective of this chapter is to understand the concept of cyber security along with its need in day to day life.
- Layered-security approach is about maintaining appropriate security measures and procedures at five different levels within your IT environment.

Theory / Practical

Theory

Duration

2 Hours

Latest Technological Trends

1. Introduction to IoT
2. How the Internet of Things (IoT) Is Changing the Cybersecurity Landscape?
3. Threats and Countermeasures of IoT and BYOD
4. Cyber security concerns and solution in Smart City & Home Automation

Objective

- By including IoT and BYOD student will get into insight of latest technological advancement in Cyber security as well as in technology. Also student will understand cyber security is playing vital roll in these technology by pointing threats.

Theory / Practical

Theory

Duration

1 Hour

Basics of Networking

1. GET MAC,NCPA.CPL, cmd line
2. Obtaining IP address from DHCP Server
3. IP address: types of IP’s, Classes of IP’s.
4. IPV4 and IPV6 address
5. Sharing Files and Folders

Objective

- To get familiarize with an OS and its Basic Settings, File management in OS
- To learn the comparison between Linux and Windows

Theory / Practical

Theory and Practical

Duration

4 Hours

Introduction to virtualization and installation of OS on virtual Box.

1. Introduction to virtualization.
2. Installation of virtual box
3. Installation of OS.

Objective

- To get introduced to virtual application system and the sequence of booting file.
- To learn basic concepts of networking

Theory / Practical

Duration

Module 2

Introduction to Cyber Security

1. What is password?
2. Types of passwords :
   - BIOS password.
   - System password :
     -- Administrator password.
     -- User password.
3. Passwords storage – windows and Linux.
4. Types of passwords attacks.

Objective

- This chapter will give complete idea of Passwords and are extremely important aspect of security policy. They are the front line of protection for user accounts.
- How one can safeguard his system by setting strong password

Theory / Practical

Theory and Practical

Duration

3 Hours

Web browser Security

1. Understanding web browsers.
2. Security features of different web browsers.

- Internet Explorer.
- Google Chrome.
- Firefox Mozilla.
- Opera.

Objective

- This chapter will give complete understanding of web browsers.
- This will explain security settings and features of different web browsers which will be very useful for users to secure his web browsing activities.

Theory / Practical

Theory and Practical

Duration

2 Hours

Firewall And UTM

1. Understanding the Firewall.
2. What exactly Unified Threat Management Is?
3. Use of Firewall and UTM.
4. Advantages and Disadvantages of UTM.

Objective

- This chapter covers the firewall as a security measure and its types.
- Different firewall techniques which are useful for data protection. One can select the technique as per own requirement.
- UTM is single hardware platform blended with layers of threat protection.
- Protect your network using multi-layered proven protection technologies including Advanced Threat Protection (ATP), IPS, VPN, email and web filtering combined with the industry’s simplest admin interface.

Theory / Practical

Theory

Duration

1 Hour

Module 3

Physical Security

1. Understanding physical security
2. Need for physical security.
3. Physical security equipments :
   - Close circuit television cameras (CCTV) : -- Analogue cameras.
     -- Digital cameras.
   - Biometrics :
     -- Fingerprint.
     -- Iris.
     -- Retina.
     -- Face.
     -- Security
     tokens. -- Smart
     card.

Objective

- The objective of this chapter is to understand physical security and its need.
- For application of physical security we are going to study some security equipments like CCTV cameras and biometrics system.
- This will help to implement physical security in any organization.

Theory / Practical

Theory

Duration

1 Hour

Mobile Security

1. Different Mobile platforms.
2. Mobile security features.
3. Applications of mobile security.
4. Different security options in mobile like encryption etc.

Case studies.

Objective

- This chapter covers different mobile platforms. Different applications used for mobile security.
- How to create mobile hotspots.

Theory / Practical

Theory and Practical

Duration

2 Hours

Module 4

Email Security

1. What is E-mail?
2. Understanding how Email works.
3. Types of Email.
4. Email Security :
   - How to set up spam filters?
   - Prevent yourself from phishing.
   - Use encryption.

Keep your computer updated.

Objective

- This chapter covers details of electronic mail.
- How E-mail works and its types.
- E-mail Tracing includes how to identify fake mail through Email header analysis.
- Email security includes how to secure emails by setting spam filters, by using encryption etc.

Theory / Practical

Theory and Practical

Duration

4 Hours

Module 4

Malware

1. What are Malwares?
2. Different types of Malwares like viruses, Worms, Trojans, Adwares, Spywares.
3. Ransomware Rootkits, and Keyloggers etc.
4. How to secure system from malware?

Objective

- In this topic students will be able to understand different types of malwares.
- This chapter includes very important area that how to secure yourself from Malwares?

Theory / Practical

Theory and Practical

Duration

2 Hours

Module 5

Cryptography

1. Understanding cryptography
2. Goals of cryptography
3. Cryptographic methods :
   - Rotation
   - Substitution :
     -- Mono-alphabetic substitution. -
     - Poly-alphabetic substitution.
   - Transposition.
4. Types of cryptography :
   - Symmetric key cryptography.
   - Asymmetric key cryptography.
5. Use of Hash function in cryptography.

Digital Signature in cryptography.

Objective

- The objective of this chapter is to understand the science of cryptography.
- In cryptography we will cover security along with cryptographic methods and types of cryptography.

Theory / Practical

Theory and Practical

Duration

3 Hours

Module 6

Wireless Security

1. Concept of Wireless Networks
2. Security Features of WiFi
3. Wireless Encryption Protocols :
   - WEP
   - WPA
   - WPA2
4. Wireless Attacks and Countermeasures

Objective

- Wireless Security will be given an insight view of wireless networks and their security parameters to the students.

Theory / Practical

Theory and Practical

Duration

2 Hours

Module 7

Ethical Hacking

1. Concept of Ethical Hacking.
2. Ethical hacking steps.
   - Reconnaissance :
   -- Active reconnaissance.
   -- Passive reconnaissance.
   - Scanning :
   -- Port scanning.
   -- Network scanning.
   -- Vulnerability scanning.
   - Gaining Access.
   - Maintaining Access.
   - Covering Tracks.

Objective

- The objective of this topic is to understand the difference between hacking and ethical hacking.
- How ethical hacking is used for security purpose.
- In this chapter we are going to cover steps of ethical hacking in detail.

Theory / Practical

Theory and Practical

Duration

4 Hours

Module 8

Virtualization and Cloud Computing

1. Basic Concept of Virtualization
   - Types of Virtualization
   - Benefits
2. Data Center Virtualization
3. Desktop Virtualization
4. Virtualizing Enterprise Application
5. Network Virtualization
6. Server Virtualization
7. Load Balancing with Virtualization

Cloud computing :

1. Definition of cloud
2. Cloud Architecture
3. Advantages of cloud
4. Risks involved in cloud computing.
5. Cloud Storage
6. Cloud Services :
   - Software As Service (SAS)
   - Platform As Service (PAS)
   - Infrastructure As A Service
7. Public Cloud Environment

Objective

- Virtualization is latest technology. With knowledge of Virtualization, one physical server can be made to act as many virtual servers. It offers a range of benefits, which is reducing the number of physical servers an organization needs.
- Cloud computing is a general term for anything that involves delivering hosted services over the Internet, Distributed Computing.
- With this chapter, student will clear with concept, Requirement, Application of cloud.

Theory / Practical

Theory and Practical

Duration

2 Hours

Module 9

Cyber Crime and Cyber Laws

1. What are cyber-crimes?
2. Types of cyber-crimes.
    - Password related crimes
    - Email related crimes
    - Desktop related crimes
    - Social networking sites related crimes
    - Website related crimes
    - Network related crimes.

Social engineering related crimes

1. Categories of Cyber Crime
    - Individual
    - Property
    - Government
2. Online Banking
    - Online banking frauds

Safety tips for online banking

Objective

- This chapter will educate the students regarding
- Cyber-crimes related to day to day activity of students on internet.
- Different categories of cyber-crimes and how one should be careful while handling the internet.
- How One should be careful while doing online banking.

Theory / Practical

Theory

Duration

1 Hours

Cyber laws (Information Technology Act 2000)

1. What is cyber law?
2. Evolution of cyber law in India.
3. Jurisdiction of IT Act
4. Penalties under IT Act.
5. Difference between civil law and criminal law
6. Offences under IT Act- some sections : Section 43, Section 65, Section 66, Section 67, Section 72, Section 69, Section 79.
7. Intellectual Property Rights (IPR).

Objective

- Through this chapter students will understand what cyber laws are and how different sections are applicable for different cyber-crimes.
- By teaching cyber laws we try to create awareness among students regarding penalties under different sections.

Theory / Practical

Theory

Duration

1 Hours

Module 10

ISO 27001

1. Introduction to ISO 27001
2. General requirements for ISO standardization.
   - Methodological requirements
   - Security control requirements.
3. Different corporate policies.

Implementation and establishment of ISMS

Objective

- This chapter will cover ISO standardization for information security.
- For any size of company which are the general requirements to take ISO standard.
- How to establish and implement information security management system

Theory / Practical

Theory

Duration

1 Hour

Module 11

IP based communication: (VOIP)

1. Introduction
2. How VoIP worked?
3. Requirements, Availability and
4. Service Limitation
5. Threat or Risk
6. Countermeasures
7. Media gateway control
8. Protocol
9. SIP (Session Initiation Protocol)

Objective

- It is new technology that improves
- Internet communication.
- This topic will brief on its function & some of its Application like Skype etc.

Theory / Practical

Theory

Duration

1 Hour

Module 12

Protection of information Assets BC/DR Planning & Development

1. Explain Disaster.
2. Types of Disaster.
3. Risks Involved.
4. Disaster recovery.
5. BCDR Plan Steps
6. Basic of Business Continuity Plan
7. Benefits of BCP and DRP Planning
8. BCP Process Steps
9. Development of Business Continuity Plan

Objective

- The objectives of a business continuity plan (BCP) are to minimize financial loss to the institution; continue to serve customers and financial market participants.
- Also on development model this chapter focused on how to get the business up and running in the event that a specific facility or function is disrupted, rather than on the precise nature of the disruption.

Theory / Practical

Theory

Duration

2 HourS

Total - 40 Hours

Skills Factory Learning Pvt. Ltd.

Ph no. 020 25451488, 25464656

Web : www.skills-factory.com

List of topics -Digital Ethical Hacking certificate course

1) **Certificate in Digital Ethical Hacking-**

1. Introduction to Hacking, 2. Information Gathering / Vulnerability Scanning,3. Malwares (Virus, Worm, Trojan…), 4. System Hacking, 5. Sniffing, 6. Site and Web server Hacking, 7. SQL Injection and Cross Site Scripting, 8. Buffer Overflow, 9. Multi-Platform (cross-platform) System Hacking 10. Mobile Pentesting ,11. Network DOS and DDOS, 12. Cryptography, Penetration Testing IDS / IPS and Firewall

Sr No	Formal structure of the Course
1	Introduction to Hacking
2	Information Gathering / Vulnerability Scanning
3	Malwares (Virus, Worm, Trojan…)
4	System Hacking
5	Sniffing
6	Site and Web server Hacking
7	SQL Injection and Cross Site Scripting
8	Buffer Overflow
9	Multi-Platform (cross-platform) System Hacking and
10	Mobile Pen testing
11	Network DOS and DDOS
12	Cryptography
13	Penetration Testing IDS / IPS and Firewall
14	Make reports based on test results and make enhancements to existing security solutions
15	Manage your work to meet requirements
16	Work effectively with colleagues
17	Maintain a healthy, safe and secure working environment

Digital Ethical Hacking Course Curriculum

Add - on

Networking

1.\ Introduction to Networking
2.\ OSI Model
3.\ TCP/IP Vs. OSI Model
4.\ Protocols
5.\ IP address Vs. MAC address

Objective

- Understanding of basic networking terminologies, topologies, protocols and addressing scheme.

Theory / Practical

Theory

Duration

5 Hours

Model 1

Introduction to Hacking

1.\ Introduction To Hacking
2.\ Essential Terminology
3.\ Confidentiality Integrity Availability (C.I.A)
4.\ Types of Hacker
5.\ Types of System Attack
6.\ Impact of Hacking

Objective

- Understanding of Information Security and essential terminology used in Ethical Hacking.

Theory / Practical

Theory

Duration

2 Hours

Model 2

Information Gathering/ Vulnerability Scanning

1.\ Footprinting Concepts
2.\ Footprinting Methodology
3.\ Footprinting through Social Networking Sites
4.\ Email Footprinting
5.\ WHOIS Footprinting
6.\ Network Scanning
7.\ Scanning Techniques
8.\ Scan for Vulnerability
9.\ Vulnerability Assessment
10.\ Network Vulnerability Scanning
11.\ Vulnerability Scanning for Mobile

Objective

- Techniques of Gathering information about potential target. Finding Weak areas of target for exploitation. Scanning and classification of vulnerability found.

Theory / Practical

Practical

Duration

3 Hours

Model 3

Malwares (Virus,Worm,Trojan…)

1. Introduction to Malware
2. Concepts of Virus,Worm,Trojan
    5. Types of Trojans
    6. Types of Virus and Worms
    7. Malware Reverse Engineering
    8. Penetration Testing

Objective

- Insight of Malware Learn how to detect and quantify Virus,Worm,Trojan and other types of malware. Reverse engineering of Malware codes

Theory / Practical

Practical

Duration

3 Hours

Model 4

System Hacking

1. System Hacking Goals
2. Methodology
5. Password Cracking
6. Key loggers
7. Spyware
8. Covering Tracks

Objective

- Understanding the process of exploiting vulnerabilities, password cracking, post exploitation and clearing tracks

Theory / Practical

Practical

Duration

3 Hours

Model 5

Sniffing

1. What is Sniffing?
2. Types of Sniffing
6. IP Spoofing
7. MAC Spoofing
8. DHCP Hijacking
9. ARP Poising
10. DNS Poising
11. Network Sniffing
12. Online credential sniffing and countermeasures
13. Sniffing Detection
14. Web Sniffing and patching

Objective

- Understanding of Network sniffing and packet spoofing. Tools used for network stress testing

Theory / Practical

Practical

Duration

3.5 Hours

Model 6

Web Site and Web server Hacking

1. Webserver Attacks
2. Attack Methodology
3. Webserver Footprinting Tools
4. Enumerating Webserver Information
4. Webserver Attack
5. Metasploit
6. Webserver Security
7. Web Server Security Scanner
8. SQL Injection Attacks
9. Cross-Site Scripting (XSS) Attacks
10. Cross-Site Request Forgery (CSRF) Attack
11. Session Fixation Attack
12. Cookie/Session Poisoning
13. Buffer Overflow Attacks
14. CAPTCHA Attacks
15. Improper Error Handling
16. Web Services XML Poisoning
17. Web App Hacking Methodology
18. Attacking Web Servers
19. Analyze Web Applications
20. Attack Authentication Mechanism
21. Authorization Attack Schemes
22. Attack Session Management Mechanism
23. Perform Injection Attacks
24. Web Application Hacking Tools

Objective

- Advanced Web site and Web server attack methods and configuration vulnerability. Advanced XSS and CSRF attack with advanced SQL injection. Identifying weak configuration and quantifying the founded vulnerabilities. Uses of Web Application Pen testing tools.

Theory / Practical

Practical

Duration

3.5 Hours

Model 7

SQL Injection and XSS

1. SQL Injection
2. Types of SQL Injection
3. SQL Injection Attacks
4. Advanced SQL Injection

- SQL Injection Counter-measures
- Cross-Site Scripting (XSS) Attacks
- Cross-Site Scripting Attack Scenario
- Advanced XSS Attack
- Cross-Site Request Forgery (CSRF) Attack

Objective

- Web Application hacking with XSS and SQL injection. Advanced tools used for attacking sophisticated security environment on web servers as well as code level attacks on front end of web application or website. Quantifying and applying security practices

Theory / Practical

Practical

Duration

4 Hours

Model 8

Buffer Overflow

- Buffer Overflows: Attacks and Defences for the Vulnerability of the Decade
- Basic Integer Overflows
- Exploiting Format String Vulnerabilities
- Stack based Buffer overflow
- Heap Based Buffer Overflow

Objective

- Buffer overflow attack scenario and exploitation for good. And to find possible breach

Theory / Practical

Practical

Duration

3 Hours

Model 9

Cross Platform System Hacking and Wireless Hacking (Linux/Windows/Server)

1. Hacking Methodology
2. Exploiting Bugs in Linux / Windows
3. Stress testing of Operating system

- Fuzzing
- Network Hacking
- Bypassing Authentication
- Exploiting Operating system level vulnerabilities
- Exploit identification and Payload Management

Objective

- Cross Platform hacking and exploiting possible vulnerabilities in popular operating system platform. Understanding 802.11 weakness, WEP cracking, de-authentication and its countermeasures.

Theory / Practical

Practical

Duration

4 Hours

Model 10

Mobile Pentesting

1. Hacking Android OS
2. Android Trojan
3. Securing Android Devices
5. Hacking iOS
6. Jailbreaking iOS
7. Securing iOS Devices
8. Mobile Device Management (MDM)
9. Bring Your Own Device (BYOD)
10. Mobile Penetration Testing

Objective

- Mobile penetration testing. Hacking into Android, Windows and iOS platform to find possible vulnerabilities in native code as well as in app based structure

Theory / Practical

Practical

Duration

3 Hours

Model 11

Network DOS and DDOS

1. DoS/DDoS Attack
2. Botnets, Zombies

- DoS/DDoS Attack Tools
- Attack Forensics
- Enabling TCP Intercept
- DoS/DDoS Protection Tools
- DoS/DDoS Attack Penetration Testing
- Mitigate Attacks
- Deflect Attacks
- Application Level Flood Attacks

Objective

- Network pentesting and sterss testing with advanced Dos and DDoS attacks.

Theory / Practical

Practical

Duration

4 Hours

Model 12

Cryptography

1. Cryptography
2. Encryption Algorithms
4. Cryptography Advantages
5. Ciphers
6. Data Encryption Standard (DES)
7. Advanced Encryption Standard (AES)
8. RC4, RC5, RC6 Algorithms
9. RSA
10. Public Key Infrastructure(PKI)
11. Disk Encryption

Objective

- Understanding of Cryptography and its data hiding techniques with latest algorithms and possible tools

Theory / Practical

Duration

4 Hours

Model 13

Penetration Testing IDS/IPS and Firewall

1. Penetration Testing Methodology
2. Network Penetration testing
5. Application Penetration Testing
6. Report Generation

Objective

- Penetration Testing methodology and area of deployment as well as a effective Report creation

Theory / Practical

Practical

Duration

3 Hours

Total - 45 Hours

Skills Factory Learning Pvt. Ltd.
Ph no. 020 25451488, 25464656
Web : www.skills-factory.com