Cybersecurity Course Curriculum by 10Pie

👉 Whether you want to start your IT career or looking for guidance on how to plan your future career path, 10Pie is your learning hub for tech career knowledge.

Here’s a cyber security course syllabus at a glance:

Sl.No	Module Name	Topics Covered	Cybersecurity projects to Practice
1	**Advanced Network Security**	Network architecture, protocols, segmentation, vulnerabilities, firewalls, IDS/IPS, security policies, incident response	- Configure a firewall to block specific traffic patterns using pfSense or Cisco ASA. - Conduct a network vulnerability scan using Nessus or OpenVAS.
2	**Cryptography and Access Control**	Cryptosystems, symmetric/asymmetric cryptography, key management, access control models, IAM	- Implement a Public Key Infrastructure (PKI) using OpenSSL or Microsoft Certificate Services. - Configure a VPN using OpenVPN or Cisco AnyConnect.
3	**Web Application Security**	HTTP/HTTPS protocols, web vulnerabilities (SQL injection, XSS), secure coding practices, WAFs	- Conduct a web application vulnerability scan using OWASP ZAP or Burp Suite. - Develop a secure web application using OWASP ESAPI or Spring Security.
4	**Cloud Security**	Cloud deployment/service models, security risks, compliance frameworks, incident response	- Configure a cloud security group using AWS Security Groups or Azure Network Security Groups. - Perform a cloud security assessment using AWS IAM Access Analyzer.
5	**Endpoint Security**	Endpoint security architecture, threats (malware, ransomware), endpoint security solutions	- Configure a host-based intrusion detection system (HIDS) using OSSEC or Samhain.

			- Develop a custom endpoint security policy using Group Policy.
6	**Incident Response and Digital Forensics**	Incident response methodologies, planning, digital forensics fundamentals	- Build an incident response plan using NIST 800-61. - Practice incident response techniques using CISA’s Cybersecurity Exercises.
7	**Security Operations and Log Management**	SOC design, log collection/analysis, SIEM systems	- Implement a SIEM system using Splunk or ELK Stack. - Configure log collection using Logstash or Graylog.
8	**Identity and Access Management**	IAM fundamentals, access control models, IAM in the cloud	- Implement an IAM solution using Okta or Azure Active Directory. - Configure a single sign-on (SSO) solution using OneLogin.
9	**Mobile Device Security**	Mobile device security overview, threats, security solutions	- Implement a mobile device management (MDM) solution using Microsoft Intune. - Develop a custom mobile device security policy using Apple Configurator.
10	**Security Frameworks and Compliance**	Security frameworks (NIST, ISO 27001), compliance requirements	- Implement a security framework like NIST Cybersecurity Framework. - Conduct a compliance assessment using HIPAA Security Rule.
11	**Defensible Network Architecture**	Network architecture design, security risks, controls, monitoring	- Design a defensible network architecture diagram. - Implement network security controls using virtual machines.
12	**Protocols and Packet Analysis**	Network protocols, packet analysis (tcpdump, Wireshark), security risks, best practices	- Capture live network traffic using Wireshark. - Utilize tcpdump to analyze captured packets.

13	**Cybersecurity Governance and Risk Management**	Risk assessment methodologies, threat modeling, compliance requirements	- Conduct a risk assessment for a hypothetical organization. - Create a mock implementation plan for a cybersecurity governance framework.
14	**Cybersecurity Analytics and Intelligence**	Cybersecurity analytics fundamentals, threat intelligence lifecycle, data analysis techniques	- Collect and analyze threat intelligence data. - Simulate a threat hunting scenario using network logs.
15	**Cybersecurity Incident Response and Disaster Recovery**	Incident response planning, disaster recovery in the cloud	- Draft an incident response plan for a ransomware attack. - Conduct a tabletop exercise to simulate a cybersecurity incident.

Module 1: Advanced Network Security

Network architecture and design

- Network topology and protocols
- Network segmentation and isolation
- Network virtualization and SDN

Network protocols and vulnerabilities

- TCP/IP protocol suite
- DNS and DHCP security
- IPv6 security considerations
- Network protocol vulnerabilities (e.g. DNS amplification attacks)

Firewalls and intrusion detection systems

- Firewall types (packet filtering, stateful inspection, application-layer)
- Firewall configuration and management
- IDS/IPS systems and signatures
- Next-generation firewalls (NGFWs)

Network security policies and procedures

- Network security policy development and implementation
- Network access control (NAC) and authentication
- Network segmentation and isolation policies
- Incident response and disaster recovery planning

Secure communication protocols

- SSL/TLS protocol and certificate management
- IPsec protocol and implementation
- Secure Shell (SSH) and Secure File Transfer Protocol (SFTP)
- Email security protocols (e.g. PGP, S/MIME)

⭐ Hands-on projects to practice:

- Configure a firewall to block specific traffic patterns using a tool like pfSense or Cisco ASA.
- Implement a Network Access Control (NAC) system using a tool like Cisco ISE or ForeScout.
- Conduct a network vulnerability scan using a tool like Nessus or OpenVAS.

Module 2: Cryptography and Access Control

Cryptosystem fundamentals

- Symmetric and asymmetric cryptography
- Hash functions and digital signatures
- Cryptographic algorithms (e.g. AES, RSA, ECC)
- Key management and exchange

Cryptography algorithms and deployment

- Block ciphers and modes of operation
- Public-key cryptography and certificate authorities
- Digital certificates and public key infrastructure (PKI)
- Cryptographic protocols (e.g. SSL/TLS, IPsec)

Digital signatures and certificates

- Digital signature schemes (e.g. RSA, ECDSA)
- Certificate authorities and trust models
- Certificate revocation lists (CRLs) and online certificate status protocol (OCSP)
- Code signing and digital rights management

Access control models

- Mandatory access control (MAC)
- Discretionary access control (DAC)
- Role-based access control (RBAC)
- Attribute-based access control (ABAC)

Identity and access management

- Identity management systems (e.g. LDAP, Active Directory)
- Authentication protocols (e.g. Kerberos, NTLM)
- Authorization and access control mechanisms
- Identity and access management in the cloud

⭐ Hands-on projects to practice:

- Implement a Public Key Infrastructure (PKI) using a tool like OpenSSL or Microsoft Certificate Services.
- Configure a VPN using a tool like OpenVPN or Cisco AnyConnect.
- Implement role-based access control (RBAC) using a tool like Active Directory or LDAP.

Module 3: Web Application Security

Web communication fundamentals

- HTTP and HTTPS protocols (SSL/TLS encryption, certificate management, handshake, validation, and security best practices)
- HTML, CSS, and JavaScript security considerations
- Web application architecture and design

Web application vulnerabilities

- OWASP web application security risks
- SQL injection and cross-site scripting (XSS)
- Cross-site request forgery (CSRF) and clickjacking
- Input validation and sanitization

Secure coding practices

- Secure coding guidelines and best practices
- Input validation and error handling
- Secure coding for web applications (e.g. OWASP ESAPI)
- Code reviews and secure coding assessments

Web application firewalls and security information and event management

- Web application firewall (WAF) configuration and management
- Security information and event management (SIEM) systems
- Log analysis and incident response
- Web application security monitoring and analytics

Secure web development frameworks and libraries

- Secure web development frameworks (e.g. Ruby on Rails, Django)

- Secure web development libraries (e.g. OWASP ESAPI)
- Web application security testing and validation

⭐ Hands-on projects to practice:

- Conduct a web application vulnerability scan using a tool like OWASP ZAP or Burp Suite.
- Implement a web application firewall (WAF) using a tool like ModSecurity or AWS WAF.
- Develop a secure web application using a framework like OWASP ESAPI or Spring Security.

Module 4: Cloud Security

Cloud computing fundamentals:

- Cloud deployment models (public, private, hybrid)
- Cloud service models (IaaS, PaaS, SaaS)
- Cloud security architecture and design

Cloud security risks and threats:

- Data breaches and unauthorized access
- Malware and ransomware in the cloud
- Denial of service (DoS) and distributed denial of service (DDoS) attacks
- Cloud security risks and threats (e.g. AWS, Azure, Google Cloud)

Cloud security controls and compliance:

- Cloud security controls and compliance frameworks (e.g. CSA, NIST)
- Cloud security auditing and assessment
- Cloud security governance and risk management
- Cloud security standards and regulations (e.g. PCI-DSS, HIPAA)

Cloud security monitoring and incident response:

- Cloud security monitoring and logging
- Cloud incident response and disaster recovery planning
- Cloud security analytics and threat intelligence
- Cloud security incident response and remediation

⭐ Hands-on projects to practice:

- Configure a cloud security group using a tool like AWS Security Groups or Azure Network Security Groups.
- Implement a cloud access security broker (CASB) using a tool like Netskope or Skyhigh Networks.

- Perform a cloud security assessment using a tool like AWS IAM Access Analyzer or Azure Security Center.

Module 5: Endpoint Security

Endpoint security overview

- Definition and importance of endpoint security
- Types of endpoints (laptops, desktops, mobile devices, servers)
- Endpoint security architecture and components

Endpoint security threats

- Malware (viruses, Trojans, spyware, adware)
- Ransomware (types, attack vectors, and mitigation strategies)
- Phishing (types, tactics, and defense mechanisms)
- Advanced Persistent Threats (APTs) and targeted attacks
- Zero-day exploits and unknown threats

Endpoint security solutions

- Antivirus software (signature-based, behavioral, and cloud-based)
- Anti-malware tools (detection, removal, and prevention)
- Endpoint Detection and Response (EDR) solutions
- Host-based Intrusion Detection Systems (HIDS)
- Endpoint security suites and integrated solutions

⭐ Hands-on projects to practice:

- Configure a host-based intrusion detection system (HIDS) using a tool like OSSEC or Samhain.
- Develop a custom endpoint security policy using a tool like Group Policy or PowerShell.

Module 6: Incident Response and Digital Forensics

- Incident response methodologies (NIST, SANS)
- Incident response planning and preparation
- Digital forensics fundamentals (data acquisition, analysis, reporting)
- Incident response and digital forensics tools (EnCase, FTK, X-Ways)
- Incident response and digital forensics in the cloud

⭐ Hands-on projects to practice:

- Build an incident response plan using a framework like NIST 800-61 or SANS Incident Response.

- Practice incident response techniques using a tool like Cybersecurity and Infrastructure Security Agency (CISA)'s Cybersecurity Exercises.

Module 7: Security Operations and Log Management

- Security operations center (SOC) design and implementation
- Log collection, filtering, and analysis
- Security information and event management (SIEM) systems
- Log management and analysis tools (Splunk, ELK Stack)
- Security operations and log management in the cloud

⭐ Hands-on projects to practice:

- Implement a security information and event management (SIEM) system using a tool like Splunk or ELK Stack.
- Configure log collection and analysis using a tool like Logstash or Graylog.
- Develop a security operations center (SOC) use case using a tool like Phantom or Demisto.

Module 8: Identity and Access Management

- Identity and access management (IAM) fundamentals
- Identity management systems (LDAP, Active Directory)
- Access control models (MAC, DAC, RBAC)
- Identity and access management in the cloud (AWS IAM, Azure AD)
- Identity and access management best practices and compliance

⭐ Hands-on projects to practice:

- Implement an identity and access management (IAM) solution using a tool like Okta or Azure Active Directory.
- Configure a single sign-on (SSO) solution using a tool like OneLogin or Ping Identity.

Module 9: Mobile Device Security

- Mobile device security overview (Android, iOS)
- Security threats (malware, unauthorized access) for mobile devices
- Security solutions (MDM, MAM)
- Mobile device security monitoring and incident response

⭐ Hands-on projects to practice:

- Implement a mobile device management (MDM) solution using a tool like Microsoft Intune or VMware Workspace ONE.
- Configure a mobile application management (MAM) solution using a tool like AppDynamics or Citrix Endpoint Management.

- Develop a custom mobile device security policy using a tool like Apple Configurator or Android Enterprise.

Module 10: Security Frameworks and Compliance

- Security frameworks (NIST, ISO 27001, COBIT)
- Compliance and regulatory requirements (HIPAA, PCI-DSS, GDPR)
- Security frameworks and compliance in the cloud
- Security frameworks and compliance best practices
- Security frameworks and compliance auditing and assessment

⭐ Hands-on projects to practice:

- Implement a security framework like NIST Cybersecurity Framework or ISO 27001.
- Conduct a compliance assessment using a tool like HIPAA Security Rule or PCI DSS.
- Develop a custom security policy using a tool like PolicyStat or ComplianceForge.

Module 11: Defensible Network Architecture

- Defensible network architecture design and implementation
- Network security architecture and design
- Network security risks and threats (data breaches, unauthorized access)
- Network security controls and compliance
- Network security monitoring and incident response

⭐ Hands-on projects to practice:

- **Design a Defensible Network Architecture:** Create a comprehensive network architecture diagram for a hypothetical organization. Include segmentation, firewalls, intrusion detection systems (IDS), and access controls, while applying principles of least privilege and zero trust.
- **Implement Network Security Controls:** Set up a small-scale network using virtual machines to simulate a defensible architecture. Implement security controls such as firewalls, VPNs, and IDS/IPS. Test the effectiveness of these controls against simulated attacks to evaluate their performance.
- **Network Monitoring and Incident Response Simulation:** Use tools like Wireshark or Snort to monitor network traffic in your simulated environment. Create incident response playbooks for various scenarios (e.g., detecting a data breach) and practice executing these plans based on real-time alerts and logs.

Module 12: Protocols and Packet Analysis

- Network protocols and vulnerabilities
- Packet analysis fundamentals (tcpdump, Wireshark)
- Protocol analysis and troubleshooting

- Network protocol security risks and threats
- Network protocol security best practices and compliance

⭐ Hands-on projects to practice:

- **Network Traffic Analysis with Wireshark**: Capture live network traffic using Wireshark, apply filters to isolate specific protocols (like HTTP or DNS), and analyze the data to identify anomalies or vulnerabilities.
- **Packet Capture and Analysis:** Utilize tcpdump to capture packets from a specific interface, then analyze the captured data using Wireshark to understand the packet flow and identify potential security risks.
- **Protocol Troubleshooting Simulation:** Create a simulated network environment where you intentionally misconfigure protocols (e.g., incorrect DHCP settings) and use packet analysis tools to troubleshoot and resolve the issues.

Module 13: Cybersecurity Governance and Risk Management

- **Risk Assessment Methodologies:** NIST 800-30, FAIR, OCTAVE, and other risk assessment methodologies, including their strengths, weaknesses, and applications.
- **Threat Modeling:** Identifying and analyzing potential threats to an organization's assets, including threat actors, attack vectors, and vulnerability exploitation.
- Vulnerability Management: Identifying, classifying, prioritizing, and remediating vulnerabilities in systems, applications, and networks, including vulnerability scanning and penetration testing.
- **Compliance and Regulatory Requirements:** In-depth analysis of specific regulations and standards, such as HIPAA, PCI DSS, GDPR, and NIST 800-171, including their requirements, controls, and audit procedures.
- **Cybersecurity Frameworks**: In-depth analysis of specific cybersecurity frameworks, such as NIST Cybersecurity Framework, COBIT, and ISO 27001, including their components, implementation, and integration.
- **Risk Analysis and Evaluation:** Quantitative and qualitative risk analysis techniques, including risk matrices, heat maps, and Monte Carlo simulations, to evaluate and prioritize risks.

⭐ Hands-on projects to practice:

- **Risk Assessment Project:** Conduct a risk assessment for a hypothetical organization by identifying assets, threats, and vulnerabilities, and then develop a risk management plan that includes mitigation strategies.
- **Governance Framework Implementation:** Choose a cybersecurity governance framework (like NIST or ISO 27001) and create a mock implementation plan, detailing policies, roles, and responsibilities for compliance.
- **Cloud Security Assessment:** Evaluate the security posture of a cloud service provider by reviewing their compliance with governance standards and best practices, and propose enhancements based on identified gaps.

Module 14: Cybersecurity Analytics and Intelligence

Cybersecurity Analytics and Intelligence Fundamentals:

- Definition and importance of cybersecurity analytics and intelligence
- Cloud-based analytics and intelligence architectures
- Data collection, processing, and analysis techniques
- Machine learning and artificial intelligence in cybersecurity analytics
- Threat hunting and proactive defense strategies

Cybersecurity Threat Intelligence and Analysis:

- Types of threat intelligence (strategic, tactical, operational, technical)
- Threat intelligence lifecycle (collection, analysis, dissemination, feedback)
- Threat actor analysis (motivations, tactics, techniques, and procedures)
- Indicators of Compromise (IOCs) and threat indicator management
- Threat intelligence feeds and platforms such as LevelBlue, Federal, Bureau of Investigation, Anomali, VirusTotal, Malware hashes, etc.

⭐ Hands-on projects to practice:

- **Threat Intelligence Analysis:** Collect threat intelligence data from various sources (like VirusTotal or Anomali) and analyze it to identify trends, threat actors, and potential indicators of compromise (IOCs).
- **Machine Learning Application:** Develop a simple machine learning model to classify network traffic as benign or malicious based on labeled datasets, and evaluate its effectiveness in detecting anomalies.
- **Threat Hunting Exercise:** Simulate a threat hunting scenario where you proactively search for hidden threats within a dataset of network logs, using techniques learned in previous modules.

Module 15: Cybersecurity Incident Response and Disaster Recovery

- Cybersecurity incident response methodologies (NIST, SANS)
- Cybersecurity incident response planning and preparation
- Incident response and disaster recovery in the cloud

⭐ Hands-on projects to practice:

- **Incident Response Plan Development:** Draft an incident response plan for a specific type of cybersecurity incident (e.g., ransomware attack), detailing steps for detection, containment, eradication, and recovery.
- **Disaster Recovery Simulation:** Create a disaster recovery scenario where you simulate a data breach and execute the recovery plan, testing the effectiveness of backup systems and recovery procedures.

- **Tabletop Exercise:** Conduct a tabletop exercise with a team to simulate a cybersecurity incident, discussing roles and actions to be taken, and evaluate the response effectiveness based on predefined metrics.

B.SC cybersecurity syllabus

https://www.perplexity.ai/search/who-is-eligible-for-cybersecur-4sgY9gKZTHmYMQM8YyAscg
The BSc (Hons) in Cyber Security is a 3-year undergraduate (UG) program that provides students with a strong foundation in cybersecurity principles and practices.

The average fees for the BSc (Hons) in Cyber Security course range from INR 30,000 to 5,00,000 per annum, depending on the college and location.

Here's the BSC cyber security course curriculum:

Semester	Name	Topics
I	Fundamentals of Cyber Security	Introduction to Cyber Security, Cybercrime, Network Security, Operating System Security, and Cryptography
II	Programming for Cyber Security	Introduction to Programming-I, Web Designing-I, algorithms, overview of C language, operators, decision making, branching statements, and looping statements
III	Cyber Security Threats and Vulnerabilities	Cyber Security Threats, Vulnerabilities, Risk Management, and Compliance
IV	Cyber Security Architecture and Design	Cyber Security Architecture, Design Principles, Secure Coding Practices, and Secure Communication Protocols
V	Cyber Security Operations and Management	Cyber Security Operations, Incident Response, Disaster Recovery, and Cyber Security Governance
VI	Cyber Security Project and Internship	Cyber Security Project, Internship, and Research Methodologies

B.Tech cybersecurity syllabus

The B.Tech in Cyber Security is a 4-year undergraduate program that helps students gain essential skills to protect systems and networks from cyber threats. Candidates must complete their 12th grade with a minimum of 45-60% marks, including Mathematics.

Here is the B.Tech Cybersecurity syllabus semester-wise.

Semester	Course Code	Course Title	Topics
1	CS501	Advanced Computer Networks	Network fundamentals, protocols, and architectures, Network security threats and vulnerabilities, Network security protocols and technologies
	CS502	Cryptography and Network Security	Introduction to cryptography, Symmetric and asymmetric encryption, Digital signatures and hash functions, Network security protocols (SSL/TLS, IPsec, etc.)
	CS503	Operating System Security	Operating system security principles, Access control and authentication, File system security, Windows and Linux security
	CS504	Cybersecurity Fundamentals	Introduction to cybersecurity, Cybersecurity threats and vulnerabilities, Cybersecurity frameworks and standards, Cybersecurity policies and procedures
2	CS505	Penetration Testing and Vulnerability Assessment	Penetration testing methodologies, Vulnerability assessment and management, Penetration testing tools and techniques, Reporting and documentation
	CS506	Incident Response and Disaster Recovery	Incident response methodologies, Disaster recovery planning and implementation, Business continuity planning, Crisis management and communication
	CS507	Cybersecurity Governance and Compliance	Cybersecurity governance and risk management, Compliance and regulatory requirements, Cybersecurity policies and procedures, Auditing and compliance
	CS508	Research Methodology and Academic Writing	Research methodology and techniques, Academic writing and publishing, Research ethics and plagiarism
	CS509	Advanced Cybersecurity Topics	Advanced persistent threats (APTs), Cyber-physical systems security, Internet of Things (IoT) security, Artificial intelligence and machine learning in cybersecurity

	CS510	Cybersecurity Analytics and Visualization	Cybersecurity analytics and visualization, Data mining and machine learning in cybersecurity, Security information and event management (SIEM) systems, Cybersecurity dashboard and visualization
	CS511	Cybersecurity Project Management	Cybersecurity project management methodologies, Project planning and execution, Risk management and quality assurance, Project monitoring and control
	CS512	Elective Course (Choose one)	Cloud Security, Cybersecurity in IoT, Artificial Intelligence in Cybersecurity, Cybersecurity in Blockchain
4	CS513	Project Work	Students will work on a project related to cybersecurity, Project will be evaluated based on the project report, presentation, and demonstration
	CS514	Seminar	Students will present a seminar on a topic related to cybersecurity, Seminar will be evaluated based on the presentation, content, and Q&A session

M.Tech cybersecurity syllabus

The M.Tech in Cyber Security is a 2-year postgraduate program designed for graduates holding a B.Tech, B.Sc, or equivalent degree in relevant fields.
Candidates in India must achieve a minimum of 50-60% marks in their previous degree and qualify for the GATE exam, followed by an interview.

Here is the M.Tech Cybersecurity syllabus semester-wise.

Semester 1:

Course Code	Course Title	Topics
CS501	Advanced Computer Networks	Network fundamentals, protocols, and architectures, Network security threats and vulnerabilities, Network security protocols and technologies
CS502	Cryptography and Network Security	Introduction to cryptography, Symmetric and asymmetric encryption, Digital signatures and hash functions, Network security protocols (SSL/TLS, IPsec, etc.)
CS503	Operating System Security	Operating system security principles, Access control and authentication, File system security, Windows and Linux security

CS504	Cybersecurity Fundamentals	Introduction to cybersecurity, Cybersecurity threats and vulnerabilities, Cybersecurity frameworks and standards, Cybersecurity policies and procedures

Semester 2:

Course Code	Course Title	Topics
CS505	Penetration Testing and Vulnerability Assessment	Penetration testing methodologies, Vulnerability assessment and management, Penetration testing tools and techniques, Reporting and documentation
CS506	Incident Response and Disaster Recovery	Incident response methodologies, Disaster recovery planning and implementation, Business continuity planning, Crisis management and communication
CS507	Cybersecurity Governance and Compliance	Cybersecurity governance and risk management, Compliance and regulatory requirements, Cybersecurity policies and procedures, Auditing and compliance
CS508	Research Methodology and Academic Writing	Research methodology and techniques, Academic writing and publishing, Research ethics and plagiarism

Semester 3:

Course Code	Course Title	Topics
CS509	Advanced Cybersecurity Topics	Advanced persistent threats (APTs), Cyber-physical systems security, Internet of Things (IoT) security, Artificial intelligence and machine learning in cybersecurity
CS510	Cybersecurity Analytics and Visualization	Cybersecurity analytics and visualization, Data mining and machine learning in cybersecurity, Security information and event management (SIEM) systems, Cybersecurity dashboard and visualization
CS511	Cybersecurity Project Management	Cybersecurity project management methodologies, Project planning and execution, Risk management and quality assurance, Project monitoring and control
CS512	Elective Course (Choose one)	Cloud Security, Cybersecurity in IoT, Artificial Intelligence in Cybersecurity, Cybersecurity in Blockchain

Semester 4:

Course Code	Course Title	Topics
CS513	Project Work	Students will work on a project related to cybersecurity, Project will be evaluated based on the project report, presentation, and demonstration
CS514	Seminar	Students will present a seminar on a topic related to cybersecurity, Seminar will be evaluated based on the presentation, content, and Q&A session

PG Diploma in cybersecurity syllabus

The Post Graduate Diploma in Cyber Security (PGDCS) is a 1-year program designed for graduates with a technical or science background, requiring a minimum of 60% marks.

The Cybersecurity Diploma course syllabus varies by institution, but here's a structured overview of a typical cyber security syllabus organized by semester and topics covered:

Semester I	Semester II
Introduction to Ethical Hacking	Business & Technical Logistics of Pen Testing
Linux Fundamentals	Linux Fundamentals (Advanced)
Protocols	Information Gathering (Advanced)
Cryptography	Detecting Live Systems
Password Cracking	Enumeration
Malware	Vulnerability Assessments (Advanced)
Security Devices	Malware Goes Undercover
Information Gathering – Passive Reconnaissance	Windows Hacking
Social Engineering	Hacking UNIX/Linux
Active Reconnaissance	Advanced Exploitation Techniques
Vulnerability Assessment	Pen Testing Wireless Networks
Network Attacks	Networks, Sniffing and IDS
Hacking Servers	Injecting the Database
Hacking Web Technologies	Attacking Web Technologies
Hacking Wireless Technologies	Securing Windows with PowerShell
Maintaining Access and Covering Tracks	Pen Testing with PowerShell
Project Documentation	Technical Seminar

Cyber security course subjects and topics to learn

● Understanding of networking and advanced network security

To become a cybersecurity expert, you first need to understand how data is transmitted over the internet and a few networking threats. It includes learning TCP/IP, DNS, network topologies, and OSI models. Also, you must know the network devices like routers, switches, and firewalls.

When you have the basic knowledge of networks, understanding network security becomes easy. You need knowledge of network protocol vulnerabilities like DNS amplification attacks, IPv6 security considerations, firewall and intrusion detection systems, network security policies and procedures, and different secure communication protocols. These security measures ensure the prevention of unauthorized access to the network, the detection of malicious activities, and secure communication within the network.

● Cryptography and access control

Cyber security experts must have the fundamental knowledge of cryptosystems including symmetric and asymmetric cryptography, hash functions, cryptography algorithms key management and exchange, and cryptography protocols. With cryptography you can encrypt your files and other crucial information efficiently and add confidentiality, thus, reducing the risk of exposing vital data to cyber attackers.

Knowledge of Access Control is also important and it allows you to determine who will have access to sensitive data. This includes learning Mandatory Access Control, Discretionary Access Control, Role-based Access Control, and Attribute-based Access Control. Additionally, you must learn about identity management systems, authentication protocols, authorization and access control mechanisms, and identify and access management in the cloud.

● Web application security

Knowledge of web application security helps cyber security experts secure different web applications from common vulnerabilities and threats. They first need to learn about web communication fundamentals including HTTP and HTTPS protocols, SSL/TLS encryption validation, HTML, CSS, and JavaScript security measures, and web application architecture and design.

The next thing to learn are the web application vulnerabilities including OWASP web application security risk, SQL injection and cross-site scripting, and input validation and sanitization. Additionally, you must have knowledge of secure coding guidelines and best practices, input validation and error handling, secure coding for web applications, device encryption, and more.

- ## Cloud Security

As most organizations rely on the cloud to store their vital data, security concerns are getting high. Cyber security experts must have a scheme to manage cloud environments from cyberattacks like ransomware attacks, data breaches, and denial of service attacks.

You need to start with Cloud computing fundamentals including different deployment models, Cloud service models, and Cloud security architecture and design. Additionally learn about Cloud security risks and threats, different controls and compliance frameworks, security standards and regulations, and cloud security analytics and threat intelligence.

- ## Endpoint security

Endpoint security practices protect endpoints or entry points of end-user devices like mobile devices, desktops and laptops from malicious activities and safeguard data and workflow associated with these devices. You must learn the types of endpoints, and endpoint security architecture and components before understanding different endpoint security threats like malware, ransomware, phishing, zero-day exploits, and unknown threats, and the use of tools and solutions to prevent them.

- ## Cybersecurity analytics and intelligence

With knowledge of cybersecurity analytics, you can collect and gather data for finding evidence and analyzing capabilities to perform and design effective cybersecurity strategies to detect, analyze and mitigate cyber threats. Common use cases for cyber security analytics include monitoring user behavior, identifying attempts at data exfiltration, detecting accounts that have been compromised, and identifying insider threats.

- ## Additional concepts of cybersecurity

You need to learn additional concepts of cyber security like protocols and packet analysis, defensible network architecture, security frameworks and compliance, and mobile device security, to acquire better skills in preventing systems and confidential data from cyber attacks. Additionally, you learn about incident response and management including forensic investigation and post-incident analysis, threat intelligence, and risk management and compliance.

- **Specialized cybersecurity concepts**

Once you understand the core and advanced cyber security concept you need to learn the specialized areas of cyber security. This includes penetration testing and ethical hacking, industrial control system security, cyber security for IoT, artificial intelligence in cyber security, and blockchain and cryptocurrency security.

- **Any programming language**

Having knowledge in any one programming language like Python, Java and C++ is good. It helps you write scripts, automate tasks, and understand how cyberattacks can happen on systems.

- **Linux basics**

Besides understanding Windows and MacOS, you must also learn to use and manage LINUX operating systems. This is because Linux is widely used in servers and cyber security tools. Some of the basic things to learn include common line interface, file system hierarchy, package management, and basic shell scripting.

Cybersecurity course fees and duration 2024

What is the course fee of Cybersecurity courses?

The course fee of cyber security courses ranges between ₹15,000 to ₹3,00,000. This may vary depending on several factors mainly the type of course and the course offerings. For example, if you are doing a diploma or certificate cybersecurity course, it will cost you less than a degree course like a UG or PG level course. Similarly, the institution's offerings have a great impact on the fees. A course having interview preparation, resume building, live project work, access to the latest resources, etc., charges more than ordinary courses.

Cybersecurity Course Duration

Most cyber security certificate courses range from 4 months to 1 year while degree courses may go beyond 2 years. The course duration varies depending on the type of course and the curriculum. While online or offline degree and certificate courses take longer to complete, a self-paced course gives you the flexibility to complete it within your time and learning pace.

Who is eligible for Cybersecurity courses?

If you want to enroll in any online training course for cybersecurity, there is no such criteria or eligibility. However, knowing the basics of computers, cyber networking and the internet will be helpful.

For academic courses in India: Students are eligible for cybersecurity courses after completing their 12th grade, with specific criteria depending on the course type:

- **Diploma in Cyber Security:** Open to any stream with 10+2 completion.
- **BTech in Cyber Security:** Requires 10+2 with Physics, Chemistry, and Mathematics, along with a minimum of 50% marks.
- **BSc in Cyber Security:** Eligible for students who have completed 10+2 with Mathematics, also need at least 50% marks.
- **Postgraduate Courses:** A bachelor’s degree in IT or related fields is necessary, with a minimum of 50% marks required.