

Certificate in Cyber Security

Program Description

(i) Title of the Program of Learning:

Certificate in Cyber Security

Types of qualifications: Certificate Program

Minimum credit requirement: 12 Credits

Qualification title/nomenclature: Certificate in Cyber Security

NHEQF level: 4.5

(ii) Whether allowing Single Major or Double Major or Interdisciplinary (4 year) or Multidisciplinary (3 year) UG Program(s) or 1-year PG Degree Program or 2-year PG Degree Program:

Certificate Course

(iii) Introduction of the program

The “Certificate in Cyber Security” program is designed to provide students and professionals with foundational and practical knowledge in cybersecurity, ethical hacking, cloud infrastructure security, and digital forensics. The program focuses on protecting computer systems, networks, cloud platforms, applications, and digital information from cyber threats, attacks, and unauthorized access.

The curriculum covers key areas such as network security, cloud computing security, vulnerability assessment, penetration testing, cyber attack prevention, malware analysis, cybercrime investigation, and digital evidence handling. The program combines theoretical concepts with hands-on practical training using industry-relevant cybersecurity and forensic tools.

This program is valuable for students, IT professionals, system administrators, and learners interested in developing skills for careers in cybersecurity, information security, cloud security, ethical hacking, and cybercrime investigation.

(iv) Objectives of the Program

1. To provide knowledge of cybersecurity concepts, principles, threats, vulnerabilities, and defence mechanisms.
2. To develop understanding of cloud infrastructure security, network security, and information protection techniques.
3. To introduce ethical hacking methodologies, penetration testing, and vulnerability assessment practices.

4. To provide practical exposure to cybersecurity tools, cloud platforms, and forensic investigation techniques.
5. To develop skills for identifying, analyzing, and mitigating cyber attacks and security incidents.
6. To provide knowledge of digital forensics, cybercrime investigation, and digital evidence handling procedures.
7. To prepare learners for employment opportunities, professional certifications, and entrepreneurship in the cybersecurity domain.

(v) Employment and Entrepreneurial Scope

(Benefits of studying the subject of the program)

The rapid growth of digital technologies, cloud computing, e-commerce, mobile applications, and online services has significantly increased the demand for cybersecurity professionals across industries such as banking, healthcare, education, government, telecommunications, manufacturing, and IT services.

After successful completion of the program, learners can pursue careers in the following roles:

- Cybersecurity Analyst
- Information Security Analyst
- Ethical Hacker
- Penetration Tester
- Cloud Security Associate
- SOC (Security Operations Center) Analyst
- Malware Analyst
- Cybercrime Investigation Assistant

The program also supports entrepreneurial and freelance opportunities such as:

- Cybersecurity Consultancy Services
- Security Auditing and Vulnerability Assessment Services
- Digital Forensics and Investigation Services
- Cybersecurity Awareness and Training Services
- Secure Cloud and Network Deployment Services
- Information Security Support and Monitoring Services

(vi) Learning Outcomes of the Program

After successful completion of the program, learners will be able to:

1. Understand the fundamentals of cybersecurity, ethical hacking, cloud security, and digital forensics.
2. Identify cyber threats, vulnerabilities, and security risks in computer systems, networks, cloud environments, and applications.
3. Apply security controls and countermeasures to protect digital systems and information assets.

4. Perform vulnerability assessment, penetration testing, and ethical hacking activities using cybersecurity tools and techniques.
5. Configure and manage secure network, wireless, cloud, and storage infrastructures.
6. Analyse malware behaviour, suspicious activities, and network traffic using forensic and monitoring tools.
7. Conduct digital forensic investigations including evidence acquisition, preservation, and analysis.
8. Investigate cyber incidents such as web attacks, phishing, email crimes, malware infections, and unauthorized access attempts.

(vii) Minimum Eligibility:

Class 12th Pass with Active Awareness about Information Technology and Cyber Security

Criteria for Selection of Students for Admission:

Merit on the basis of class 12th result

(viii) Permissible Number of Seats for one section: 30 Seats

Program Structure

Course Title	Course Code	L	T	P	Credits	Internal Assessment	End Term Exam	Total
Cybersecurity / Cloud Infrastructure Security		2	1		3	30	70	100
Ethical Hacking and Information Security		2	1		3	30	70	100
Digital Forensics and Cybercrime Investigation		2	1		3	30	70	100
Lab Cybersecurity / Cloud Infrastructure Security				2	1		50	50
Lab Ethical Hacking and Information Security				2	1		50	50
Lab Digital Forensics				2	1		50	50
					12	90	360	450

Scheme of Examination (Certificate in Cyber Security)

Theory:

Part A:

1. 10 Question of 2 mark each – 20 marks
2. Answer should not exceed more than 20 words
3. All questions are compulsory

Part B:

1. Any 5 Questions out of 10 Questions, of 10 marks each - 50 marks.
2. Answer should not exceed 400 words

Sessional:

There will be sessional (internal assessment) of 30 marks conducted by the department.

Practical:

Practical exams shall be conducted by one internal and one external examiner of a batch of 30 students in a day.

Duration of Practical exam is 3 hours.

A Laboratory Exercise File should be prepared by each student for each practical paper and should be submitted during practical examinations.

Practical of 50 marks distribution is as under:

- a. 30 marks for practical examination exercise for 3 questions
- b. 10 marks for Viva-voce
- c. 10 marks for Laboratory Exercise File

Eligibility:

Class 12th pass with at least 50% marks in aggregate. Admission is strictly on the basis of merit.

Venue

Department of Computer Science, MDS University Ajmer

Scheme of Examination (For Certificate in Cyber Security)

The Certificate Course in Artificial Intelligence will consist of 1 trimester of 3 months. The examination shall consist of (a) Theory papers (b) Laboratory / Practical work. Candidates will be required to pursue a regular, full-time course of study at the University department for a period of three months in order to be eligible for appearing in the examination.

1. Eligibility for Certificate in Artificial intelligence: Class 12th pass with at least 50% marks in aggregate. Admission is strictly on the basis of merit.
2. Examination:
 - i. There shall be 6 papers (3 theory and 3 practical).
 - ii. Theory paper shall be of 3 hours duration having 100 marks. Out of 100 marks 30 marks shall be considered as internal assessment based on internal test and seminars and 70 marks will be of examination at the end of each semester as determined by the University.
 - iii. The practical shall be of 50 marks assessed by external examiner.
 - iv. To pass a semester a candidate shall have to score 40% marks in each subject (theory and practical) separately and also 40% marks in aggregate of all the papers prescribed for the examination.
 - v. Due paper(s) will be applicable if a candidate obtains 40% marks in aggregate and fails in not more than one (1) paper (theory). The chance of due paper(s) will be given only thrice.
 - vi. Wherever a candidate appears at for a due paper examination he/she will do so according to the syllabus in force.
 - vii. A candidate not appearing at any examination/absent in any paper of term end examination shall be deemed as fail in that paper.
3. A candidate for a pass in the examination shall be required to obtain:
 - i. At least 40% marks in the aggregate of all the papers prescribed for the examination and
 - ii. At least 40% marks in the practical(s) wherever prescribed at the examination.

Passed with First Division 60% of the aggregate marks taken together of all the courses

Passed with second division 48%

All the rest will be declared to have passed the examination.

4. The grace marks shall be given up to 1% of the total aggregate marks of theory and practical of that semester in maximum one paper.
5. Candidates reappearing at an examination in a subsequent year shall be examined in accordance with the scheme and syllabi in force and shall be entitled to the award of the degree of year in which they clear the last failing/unclear paper.

Course 1: Cybersecurity / Cloud Infrastructure Security

Course Code:	CYSC01
Course Type:	Skill Enhancement Course
Level:	Undergraduate Foundation Level
Credits:	4 Credits
Duration:	Three months Trimester

Course Objectives:

This course provides foundational and practical knowledge in cybersecurity, cloud computing security, storage security, and network monitoring.

The program introduces learners to modern cyber defence mechanisms, secure cloud deployment models, virtualization, wireless and mobile security, storage technologies, and penetration testing concepts.

Learners will gain hands-on exposure to cloud platforms, storage systems, network monitoring tools, and cybersecurity practices used in industry environments.

Course Outcomes (COs)

After successful completion of the course, learners will be able to:

1. Understand and implement fundamental cybersecurity concepts and controls.
2. Configure and secure network, storage, and cloud infrastructures.
3. Secure wireless, mobile, and IoT environments.
4. Monitor network traffic and identify security threats.
5. Understand SQL Injection vulnerabilities and implement prevention techniques.
6. Use cybersecurity and penetration testing tools ethically in controlled environments.

Course Structure

Unit No.	Unit Title	Teaching Hours
Unit I	Network Security Fundamentals and Storage Security	15 Hours
Unit II	Cloud Computing and Wireless Device Security	15 Hours
Unit III	Data Security and Network Monitoring	15 Hours

Syllabus

Unit 1: Introduction to Computer Networks and Network Security

Introduction to Cybersecurity, Principles of Confidentiality Integrity and Availability (CIA Triad), Threats Vulnerabilities and Risks, Security Policies and Procedures, User Identification Methods, Authentication Techniques, Password-based Authentication, Multi-factor Authentication, Biometric Authentication, Authorization Models, Access Control Mechanisms, Administrative Controls. Computer network fundamentals, protocols, Security Policies, Risk Management, CCTV and Surveillance, Access Control Systems, Environmental Controls, Physical Asset Protection, Technical Controls, Firewalls, Intrusion Detection and Prevention Systems, Antivirus and Endpoint Security.

Unit 2: Cloud Computing and Wireless Device Security

Fundamentals of Virtualization, Hypervisors and Virtual Machines, Cloud Computing Concepts, Benefits and Challenges of Cloud Computing, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), Everything as a Service (XaaS), Shared Virtual Machines, Dedicated Virtual Servers, Bare-Metal Servers, Public Private and Hybrid Clouds, Wireless Standards and Protocols, Wireless Threats and Attacks, WPA WPA2 and WPA3 Security, Secure Wireless Configuration, Mobile Device Threats, Mobile Device Management (MDM), IoT Security Challenges, Securing Smart Devices and Sensors, Building Blocks of Cloud Computing including Compute, Storage, Networking, Virtualization, Security and Management Layers, Understanding the differences between IaaS PaaS SaaS and XaaS.

Unit 3: Data Security and Network Monitoring

Introduction to Cryptography, Symmetric Encryption, Asymmetric Encryption, Hashing Algorithms, Digital Signatures, Public Key Infrastructure (PKI), PKI Architecture, Digital Certificates, Certificate Authorities, SSL/TLS Concepts, Key Management, Data Classification, Data Loss Prevention, Database Security, Backup and Recovery, Secure Data Storage Practices, Network Monitoring Concepts, Packet Analysis, Introduction to SQL Injection, Types of SQL Injection Attacks, Exploitation Techniques, Detection and Prevention Methods, Secure Coding Practices, Mastering SQL Injection attacks as a common vulnerability exploited by cyber attackers, Introduction to Kali Linux, Ethical Hacking Principles, Reporting and Documentation, Using Kali Linux database penetration testing tools.

Practical / Lab Activities

Experiment 1: Encrypt a file using a password: Open a file encryption tool (like 7-Zip or VeraCrypt). Encrypt a text document using an AES-256 password and verify that the file cannot be read without the correct key.

Experiment 2: Decode an encrypted message using keys: Use an open-source tool (like GnuPG or Kleopatra) to generate a public/private key pair. Share your public key with a classmate, have them send you an encrypted note, and use your private key to decrypt it.

Experiment 3: Capture your first live network packet: Launch **Wireshark**, select your active Wi-Fi or Ethernet network interface, and click the start button. Browse to an open web page, stop the capture, and count how many total packets were recorded.

Experiment 4: Filter network traffic by protocol: Take a live Wireshark packet capture. Use the display filter bar to type dns or arp to isolate and look closely at background network naming requests.

Experiment 5: Inspect a plaintext network password: Start Wireshark and log into a deliberately unencrypted, old HTTP test website. Stop the capture, search for the HTTP POST method, and view your entered password visible in plaintext.

Experiment 6: Log into the storage management interface: Start up the **NetApp ONTAP Simulator** virtual machine. Open a web browser, log into the System Manager GUI interface, and explore the main dashboard layout.

Experiment 7: Generate a self-signed SSL certificate: Use the command line utility OpenSSL to generate a private key and a self-signed SSL certificate (.crt file) for a local test server.

Experiment 8: Install and bind an SSL certificate: Configure a local web server (like Apache or IIS) to use your generated SSL certificate. Access the page via HTTPS and observe the web browser security warning about self-signed certificates.

Experiment 9: Reconstruct a conversation from data packets: Open a pre-captured network file in Wireshark. Right-click on a TCP packet, select "Follow $\rightarrow$ TCP Stream", and read the complete text-based data exchange between the client and server.

Experiment 10: Bypass a login screen using basic SQL injection: Access a deliberately vulnerable local test website. Type ' OR 1=1 -- into the username field to bypass the authentication check and log in without a password.

Experiment 11: Run a basic vulnerability assessment scan: Boot into **Kali Linux** and launch a vulnerability scanner tool (like Nikto) via the terminal. Run a scan against a local test web server to identify missing security headers and old software versions.

Experiment 12: Configure a network port on a storage cluster: Use the NetApp ONTAP Simulator interface or command line to view active network interfaces (net int show) and assign a static IP address to a virtual network port.

Experiment 13: Create a storage aggregate (RAID group): Navigate to the storage settings in the NetApp ONTAP Simulator. Group multiple simulated spare disks together to create a secure storage aggregate layer.

Experiment 14: Provision a storage volume: Create a flexible data storage volume (FlexVol) on top of your NetApp aggregate. Set a size limit (e.g., 5 GB) and configure space guarantees to prevent the volume from running out of room.

Experiment 15: Extract data records via SQL injection: Use a vulnerable input form on a local test site to execute a UNION-based SQL injection. Force the web page to display private data rows directly from the underlying database tables on your screen.

Experiment 16: Automatically map a database using Kali Linux tools: Open the terminal in Kali Linux and run the automated tool sqlmap against a vulnerable target URL. Instruct the tool to automatically discover and list the database names present on the server.

Experiment 17: Dump table contents from a remote database: Use Kali's sqlmap tool with advanced flags (--tables --dump) to safely extract and read the user credentials table from a test database environment.

Experiment 18: Simulate a storage disk failure and recovery: Intentionally fail a simulated hard disk drive using commands inside the NetApp ONTAP Simulator. Observe how the RAID configuration protects the data, and monitor the reconstruction process after adding a new virtual spare disk.

Suggested Software and Tools

- Kali Linux
- Wireshark
- NetApp ONTAP Simulator
- Amazon Web Services (AWS)
- IBM Bluemix / IBM Cloud
- VirtualBox / VMware
- OpenSSL
- SIEM and Log Monitoring Tools

Suggested Reference Books

Computer Security Fundamentals — Chuck Easttom

Network Security Essentials — William Stallings

Cryptography and Network Security — William Stallings

Course 2: Ethical Hacking and Information Security

Course Code:	CYSC02
Course Type:	Skill Enhancement Course
Level:	Undergraduate Foundation Level (NCrF Level 4.5)
Credits:	4 Credits
Duration:	Three Months / Trimester

Course Objectives

The course aims to:

- To introduce students to the foundational principles of information security, the cybersecurity threat landscape.
- To equip students with the technical skills required to conduct reconnaissance, vulnerability assessments, and password security audits using industry-standard penetration testing tools.
- To provide a understanding of network, web application, and wireless vulnerabilities, enabling students to implement robust defensive countermeasures.
- To analyse security architectures across emerging technologies, specifically focusing on mobile platforms, IoT ecosystems, and Industrial Control Systems (ICS/SCADA).
- To master the principles of cloud security, virtualization, and identity access management for resilient, secure cloud infrastructures.

Course Outcomes (COs)

CO Code	Course Outcome
CO1	Explain the ethical hacking, cybersecurity threats and vulnerabilities.
CO2	Analyse different types of attacks, their assessment and countermeasures.
CO3	Analyse mobile device, IoT, and cloud computing security threats
CO4	Apply ethical hacking concepts responsibly within legal and ethical boundaries.
CO5	Apply penetration testing methodologies, and cybersecurity tools

Course Structure

Unit No.	Unit Title	Teaching Hours
Unit I	Information Security Fundamentals and Security Assessment	15 Hours
Unit II	Network, Web, and Wireless Security	15 Hours
Unit III	Mobile, IoT and Cloud Security	15 Hours

Syllabus

Unit 1: Information Security Fundamentals and Security Assessment

Introduction to Information Security, Principles of Confidentiality Integrity and Availability (CIA Triad), Information Security Concepts and Objectives, Cybersecurity Threat Landscape, Types of Cyber Attacks, Ethical Hacking Fundamentals, Phases of Ethical Hacking, Roles and Responsibilities of Ethical Hackers, Footprinting and Reconnaissance Techniques, Vulnerability Assessment Concepts, Information Security Threats, Malware Viruses Worms and Trojans, Insider and Outsider Threats, Risk Assessment and Risk Management, Security Policies and Compliance, Vulnerability Scanning Techniques, Vulnerability Assessment Tools, Password Cracking Concepts, Password Attack Techniques, Dictionary Attacks, Brute Force Attacks, Rainbow Table Attacks, Credential Stuffing, Password Security Best Practices, Password Countermeasures and Multi-factor Authentication.

Unit 2: Network, Web, and Wireless Security

Network Security Fundamentals, Network Level Attacks, Packet Sniffing and Spoofing, Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks, Session Hijacking, Man-in-the-Middle Attacks, DNS Attacks and Countermeasures, Firewall and Intrusion Detection Systems, Network Security Monitoring, Secure Network Design Principles, Web Application Security Fundamentals, Web Application Threats and Vulnerabilities, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), File Inclusion Vulnerabilities, Web Session Attacks, Web Wireless Attacks and Vulnerabilities, Rogue Access Points, Evil Twin Attacks, Wireless Packet Sniffing, Bluetooth and NFC Security Risks, Wireless Penetration Testing Concepts, Wireless Security Countermeasures and Best Practices.

Unit 3: Mobile, IoT and Cloud Security

Mobile Device Security Fundamentals, Mobile Platform Vulnerabilities, Android and iOS Security Threats, Mobile Malware and Spyware, Mobile Application Security Risks, Mobile Device Management (MDM), Mobile Security Countermeasures, Internet of Things (IoT) Security Fundamentals, IoT Threat Landscape, Smart Device Vulnerabilities, IoT Botnets and Device Hijacking, Securing IoT Devices and Networks, Operational Technology (OT) Security Concepts, Industrial Control Systems (ICS) and SCADA Security, OT Threats and Industrial Cyber Attacks, OT Security Countermeasures, Cloud Computing Fundamentals, Cloud Service Models Cloud Deployment Models, Cloud Computing Threats and Vulnerabilities, Data Breaches in Cloud Environments, Identity and Access Management in Cloud, Cloud Security Controls, Cloud Security Monitoring, Virtualization Security and Best Practices for Secure Cloud Infrastructure.

Practical / Lab Activities

Experiment 1: Run basic network diagnostics: Open your computer's command prompt and use the ping command on a public website (like google.com). Document the response time and how it verifies a connection.

Experiment 2: Track network packet routes: Use the tracert (or traceroute) command in the terminal to map out every router hop your data takes from your lab computer to an external server.

Experiment 3: Lookup public website registration data: Use a web-based WHOIS lookup tool to gather publicly available registration data (registrar name, creation date, and contact emails) for a popular domain.

Experiment 4: Audit personal password strength: Use a secure, web-based password strength calculator to test different password variations. Note how adding numbers, symbols, and length alters the time required to crack it.

Experiment 5: Set up multi-factor authentication (MFA): Configure a dummy or personal account to use a time-based authenticator app (like Google Authenticator). Document the multi-step login flow.

Experiment 6: Deconstruct a suspicious email: Examine a sample phishing email provided by the instructor. Highlight three classic indicators of a scam, such as mismatched sender domains, urgent deadlines, and generic greetings.

Experiment 7: Discover hidden server details (DNS lookup): Use the nslookup command in your terminal to find the IP addresses and mail servers (MX records) mapped to a specific domain name.

Experiment 8: Scan a dummy device for open ports: Use an open-source network scanner (like Nmap) to scan a designated lab target IP address. Identify which network ports are open and active.

Experiment 9: Enforce a strict local password policy: Open the Local Security Policy manager on a Windows lab machine. Configure account rules to demand a minimum length of 12 characters and an account lockout after 3 failed attempts.

Experiment 10: Run a basic web vulnerability scan: Launch an open-source web application vulnerability scanner (like OWASP ZAP) against a deliberately vulnerable local test website. Identify the low-risk flaws found.

Experiment 11: Audit local system patches: Use terminal commands or built-in system administration tools to list missing security updates and patches on a local operating system.

Experiment 12: Craft an educational phishing template: Use a text editor to write a highly convincing, realistic corporate email warning employees about a fake "mandatory password reset." Label the specific psychological triggers (like fear or authority) utilized.

Experiment 13: Simulate an administrative credential harvesting page : Download or examine a raw HTML file of a generic login page. Modify its code to point form submissions toward a local dummy logging script to understand how credential harvesting works.

Experiment 14: Analyze a malicious URL link: Use an online threat intelligence platform (like VirusTotal) to scan a suspicious web link. Analyze the security vendor reports to see how malicious domains are flagged.

Experiment 15: Run a full credentialed network vulnerability assessment: Configure and execute a network vulnerability scan using a tool like Nessus Essentials or OpenVAS against a local test machine. Generate a structured report sorting flaws by severity (Critical, High, Medium, Low).

Experiment 16: Crack a weak password hash (Dictionary attack): Create a simple text file containing a standard MD5 password hash. Use an ethical hacking tool (like John the Ripper or Hashcat) alongside a basic wordlist to crack the hash and recover the plaintext password.

Experiment 17: Extract password hashes from local memory: Run an authorized audit tool in a safe, offline environment to extract obscured password hashes from a local machine's security account manager database to see how attackers harvest offline credentials.

Experiment 18: Intercept unencrypted network traffic: Open a network packet analyzer (like Wireshark) on a local test network. Capture traffic while logging into a dummy website that uses unencrypted HTTP, and locate the plain-text password hidden inside the data packets.

Reference Books

Ethical Hacking and Countermeasures — EC-Council

CEH Certified Ethical Hacker All-in-One Exam Guide — Matt Walker

Hacking: The Art of Exploitation — Jon Erickson

The Web Application Hacker's Handbook — Dafydd Stuttard and Marcus Pinto

Penetration Testing: A Hands-On Introduction to Hacking — Georgia Weidman

IoT Security Foundation Guide — IoT Security Foundation

Security+ Guide to Network Security Fundamentals — Mark Ciampa

Cyber Security Essentials — James Graham, Richard Howard, and Ryan Olson

Suggested Software and Tools

Nmap, theHarvester, Maltego Community Edition

OpenVAS, Nessus Essentials, Nikto

John the Ripper, Hashcat, Hydra

FreelPA, privacyIDEA, KeePass

GoPhish, Social-Engineer Toolkit, King Phisher

Course 3: Digital Forensics and Cybercrime Investigation

Course Code:	CYSC03
Course Type:	Skill Enhancement
Level:	Undergraduate Foundation Level (NCrF Level 4.5)
Credits:	4 Credits
Duration:	Three Months Trimester

Course Objectives

The course aims to provide students with theoretical and practical knowledge of Digital Forensics and Cybercrime Investigation. The objectives of the course are to:

- Understand the fundamentals, principles, and methodologies of digital forensics.
- Learn the process of digital evidence collection, preservation, acquisition, duplication, and analysis.
- Understand hard disk structures, file systems, and forensic investigation techniques across multiple operating systems.
- Gain knowledge of investigating cybercrimes including web attacks, email crimes, dark web activities, and malware incidents.
- Learn network traffic analysis, and forensic reporting techniques.
- Develop awareness of legal, ethical, and professional responsibilities

Course Outcomes (COs)

CO Code	Course Outcome
CO1	Understand the fundamentals of computer and digital forensics.
CO2	Explain forensic investigation processes related to digital evidence.
CO3	Perform digital evidence acquisition and duplication using forensic tools.
CO4	Verify and preserve the integrity of digital evidence during investigations.
CO5	Analyze file systems and operating system artifacts in Windows/ Linux,
CO6	Perform analysis to identify suspicious activities and security incidents.
CO7	Investigate web attacks, email crimes, and malware-related incidents

Course Structure

Unit No.	Unit Title	Working Hours
Unit I	Computer Forensics Fundamentals and Data Acquisition	15 Hours
Unit II	Operating System and Network Forensics	15 Hours
Unit III	Cybercrime Investigation and Malware Forensics	15 Hours

Syllabus

Unit 1: Computer Forensics Fundamentals and Data Acquisition

Introduction to Digital and Computer Forensics, Fundamentals of Computer Forensics, Roles and Responsibilities of Forensic Investigators, Computer Forensics Investigation Process, Evidence Identification and Preservation, Chain of Custody Procedures, Evidence Collection and Documentation, Forensic Investigation Methodology, Understanding Hard Disks and Storage Devices, Disk Structure and Partitioning, File Systems Fundamentals, FAT FAT32 NTFS EXT and APFS File Systems, File Allocation and Metadata Analysis, Deleted File Recovery Concepts, Data Acquisition and Duplication Techniques, Disk Imaging Methods, Data Hiding Methods, Steganography Concepts, Encryption and Obfuscation Techniques, Log Manipulation and Evidence Tampering, Detection of Anti-forensics Activities, Countermeasures against Anti-forensics Techniques.

Unit 2: Operating System and Network Forensics

Operating System Basics, Windows Forensics Fundamentals, Windows Registry Analysis, Windows Event Logs, User Activity Tracking, Browser and Application Artifacts, Windows File System Analysis, Recovery of Deleted Windows Files, Linux Forensics Fundamentals, Memory and Process Forensics Concepts, Network Forensics Fundamentals, Network Traffic Analysis, Packet Capturing and Packet Analysis, Log Analysis and Event Correlation, Intrusion Detection and Incident Investigation, Email and Web Traffic Monitoring, Network Attack Investigation Techniques, Wireless Network Forensics, Investigation of Network-based Attacks and Security Incidents.

Unit 3: Cybercrime Investigation and Malware Forensics

Investigating Web Attacks, Web Server and Web Application Log Analysis, Investigation of SQL Injection and Cross-Site Scripting Attacks, Session Hijacking and Website Defacement Investigation, Browser Forensics and Web Activity Analysis, Dark Web Forensics Fundamentals, Investigating Email Crimes, Email Header Analysis, Email Spoofing and Phishing Investigation, Tracking Email Sources and Attachments, Spam and Fraud Email Investigation, Email Evidence Collection and Preservation, Malware Forensics Fundamentals, Types of Malware including Viruses Worms Trojans Ransomware and Spyware, Static and Dynamic Malware Analysis, Malware Behavior Analysis, Reverse Engineering Concepts, Malware Detection and Removal Techniques, Incident Response and Reporting.

Practical / Lab Activities

Experiment 1: Generate and Verify a Cryptographic File Hash: Use a tool like HashMyFiles or the command line (CertUtil on Windows) to calculate the MD5 and SHA-256 hash of a file.

Experiment 2: Create a Bit-Stream Image of a USB Drive: Insert a dummy USB drive and use an open-source tool like FTK Imager to create a raw (.dd) forensic copy. Verify that the SHA-1 hash of the physical drive perfectly matches the hash of the created image file.

Experiment 3: Inspect Hidden File Metadata: Download a sample image or document file. Use an online or offline Exif tool (like ExifTool) to extract hidden metadata, including the camera model, software used, creation date, and GPS coordinates.

Experiment 4: Deconstruct Email Headers to Spot Spoofing: Open the raw "View Source" headers of a suspicious email. Copy and paste the text into an analyzer (like MXToolbox) to trace the originating IP address and check if SPF, DKIM, or DMARC authentication failed.

Experiment 5: Analyze Hard Disk Partition Structures: Open a disk image using a tool like Autopsy or FTK Imager. Navigate the file system structure (FAT32 or NTFS) to identify the Master Boot Record (MBR) or GUID Partition Table (GPT) locations.

Experiment 6: Fill Out a Chain of Custody Form: Review a simulated cybercrime scene description. Fill out a formal, legally minded Chain of Custody tracking sheet documenting exactly who collected the digital evidence, when, and where.

Experiment 7: Carve and Recover Deleted Files: Load a corrupted or formatted disk image into a carving tool like Autopsy or Recuva. Recover 5 deleted JPEG or PDF files that no longer appear in the standard file directory.

Experiment 8: Extract Web Browser History Artifacts: Use a forensic browser analyzer (like BrowsingHistoryView) to extract historical artifacts from a user profile. Map out a timeline of websites visited, download histories, and search terms.

Experiment 9: Investigate the Windows Registry for USB Connections: Open a Windows Registry hive file (SYSTEM) using a registry viewer tool. Locate the USBSTOR key to identify the serial number, make, and model of every USB device plugged into that machine.

Experiment 10: Audit Windows Event Logs for Failed Logins: Use Windows Event Viewer or a log parser to filter a system's Security log. Isolate Event ID 4625 (Failed Logon) to discover brute-force attack attempts, noting the timestamps and target usernames.

Experiment 11: Track Linux Command Line History: Open a forensic image of a Linux user's home directory. Extract and read the hidden .bash_history or .zsh_history files to build a chronological timeline of terminal commands executed by a suspect.

Experiment 12: Parse Web Server Logs for SQL Injection: Open a raw Apache or Nginx web server access log file in a text editor. Use search filters to identify suspicious URL strings containing SQL characters (like ' OR 1=1 --) targeting the database.

Experiment 13: Detect Cross-Site Scripting (XSS) in Traffic Logs: Analyze a web application log file to spot an XSS attack. Locate entries where a malicious script tag (like <script>alert(1)</script>) was passed through an input field to deface the site.

Experiment 14: Hunt for Unauthorized Processes on macOS/Linux: Inspect a captured system log from a macOS or Linux machine. Filter active process logs to identify hidden or masquerading background tasks running without administrative approval.

Experiment 15: Reconstruct a Network Incident from a PCAP file: Open a network packet capture (.pcap) file in Wireshark. Filter the traffic for unencrypted protocols (like HTTP or FTP) and reconstruct a downloaded file directly from the data stream.

Experiment 16: Detect Malicious Network Beacons: Use Wireshark or Brim to analyze a long-duration network capture file. Look for repetitive, automated connections (beacons) sent to an external untrusted IP address, indicating a potential malware infection.

Experiment 17: Perform Static Malware Analysis (Hashing & Strings): Take an isolated, non-executable malware sample file. Use a tool like Pestudio or the strings command to extract plaintext words hidden inside the binary code to look for malicious IP addresses or registry keys.

Experiment 18: Run Dynamic Malware Analysis in a Sandbox: Upload a safe test malware sample to an isolated automated sandbox (like Any.Run or Hybrid Analysis). Observe the generated report to see how the malware alters system files and contacts external networks in real-time.

Reference Books

Guide to Computer Forensics and Investigations — Bill Nelson, Amelia Phillips, and Christopher Steuart

Digital Forensics with Open Source Tools — Cory Altheide and Harlan Carvey

Computer Forensics: Investigating Network Intrusions and Cybercrime — EC-Council

File System Forensic Analysis — Brian Carrier

Practical Malware Analysis — Michael Sikorski and Andrew Honig

Incident Response and Computer Forensics — Jason T. Luttgens, Matthew Pepe, and Kevin Mandia

The Basics of Digital Forensics — John Sammons

Network Forensics: Tracking Hackers through Cyberspace — Sherri Davidoff and Jonathan Ham

Learning Malware Analysis — Monnappa K A

Malware Forensics Field Guide for Windows Systems — Cameron H. Malin, Eoghan Casey, and James M. Aquilina

National Institute of Standards and Technology Digital Forensics Guidelines and Publications.