**Course – 5**

**Penetration Testing, Incident Response and Forensics**

**Penetration Testing:**

1. Definition:

- Penetration testing, also known as ethical hacking, is a simulated cyber-attack on a computer system to evaluate its security.

2. Purpose:

- Identify vulnerabilities in the system.

- Assess the effectiveness of existing security measures.

3. Types of Penetration Testing:

- Black Box Testing: Simulates an external hacker with no prior knowledge of the system.

- White Box Testing: Tester has complete knowledge of the system.

- Gray Box Testing: Partial knowledge of the system, simulating an insider threat.

4. Penetration Testing Steps:

- Planning: Define scope, objectives, and rules of engagement.

- Reconnaissance: Gather information about the target.

- Scanning: Identify live hosts, open ports, and services.

- Exploitation: Actively test for vulnerabilities.

- Post-exploitation: Assess the impact of successful attacks.

- Reporting: Document findings and recommend remediation.

**Incident Response:**

1. Definition:

- Incident Response (IR) is a structured approach to addressing and managing the aftermath of a cybersecurity incident or breach.

2. IR Lifecycle:

- Preparation: Develop an incident response plan, train personnel, and establish communication channels.

- Identification: Detect and verify the occurrence of an incident.

- Containment: Limit the damage and prevent further compromise.

- Eradication: Remove the cause of the incident.

- Recovery: Restore affected systems to normal operation.

- Lessons Learned: Evaluate the incident response and update procedures.

3. Roles in Incident Response:

- Incident Responder: Investigates and mitigates incidents.

- Incident Commander: Leads the response efforts.

- Communications Specialist: Manages internal and external communications.

**Forensics:**

1. Definition:

- Cybersecurity Forensics involves collecting, analyzing, and preserving electronic evidence to investigate and prevent cybercrime.

2. Types of Forensics:

- Network Forensics: Examines network traffic for evidence.

- Disk Forensics: Analyzes data storage devices for evidence.

- Memory Forensics: Investigates the volatile memory for artifacts.

3. Forensic Process:

- Identification: Recognize potential evidence.

- Preservation: Ensure the integrity and non-alteration of evidence.

- Collection: Gather evidence using forensically sound methods.

- Analysis: Examine and interpret the evidence.

- Documentation: Record findings for legal purposes.

4. Forensic Tools:

- EnCase: A widely used forensic investigation tool.

- Autopsy: Open-source digital forensics platform.

- Wireshark: Network protocol analyzer for network forensics.