IT Management & Audits

Practical Lab Manual

Incident Response Playbook

Practical P14

Learning Domain

Cybersecurity Incident Response

Course Learning Outcomes

CLO14: Execute incident response procedures for security events

Unit

Unit VII: IT Security & Risk Management

Time Allocation: 3 hours

Learning Mode: Hands-on (70%) + Theory (30%)

Difficulty Level: Intermediate-Advanced

Incident Response Playbook

Practical P14

Quick Reference

Practical Code	P14
Practical Name	Incident Response Playbook
Slot	T/P-14
Duration	3 hours
CLO Mapping	CLO14
Unit	Unit VII: IT Security & Risk Management
Delivery Mode	Hands-on Lab
Target Audience	Intermediate-Advanced Level
India Integration	HIGH
Screenshot Count	5 Required

Prerequisites

- Basic understanding of cybersecurity concepts (threats, vulnerabilities, attacks)
- Understanding of common threat types: malware, phishing, DDoS, ransomware
- Familiarity with Python programming (variables, functions, CLI tools)
- Python 3.8+ installed on your system
- Completion of P04 (Web Application Security Scanner) recommended
- Basic knowledge of network protocols and log analysis

Tools Required

Tool	Version	Free	Notes
Python	3.8+	✓	Required
Click	Latest	✓	CLI framework
Rich	Latest	✓	Terminal formatting
Jinja2	Latest	✓	Report templates
pip	Latest	✓	Included with Python

Learning Objectives

- ✓ Understand the NIST SP 800-61 Rev 2 Incident Response lifecycle and its four phases
- ✓ Review and interpret structured incident response playbooks for common threat scenarios
- ✓ Simulate realistic security incidents (data breach, ransomware) with interactive decision-making
- ✓ Apply severity assessment using CVSS-based scoring and business impact analysis
- ✓ Track incident timelines and evidence with chain-of-custody metadata
- ✓ Generate professional incident reports with executive summaries and actionable recommendations
- ✓ Apply India-specific incident reporting requirements (CERT-In, RBI, DPDP Act)

What You Will Learn

By the end of this practical, you will:

1. Understand the complete NIST Incident Response lifecycle (Preparation, Detection & Analysis, Containment, Eradication & Recovery, Post-Incident Activity)
2. Review five structured playbooks covering data breach, ransomware, phishing, DDoS, and insider threat scenarios
3. Map playbook sections to the NIST IR lifecycle phases
4. Execute interactive incident simulations with scored decision points
5. Analyze incident timelines and track digital evidence with proper chain-of-custody
6. Calculate incident severity using CVSS-based scoring with business impact estimates
7. Generate professional HTML incident reports suitable for stakeholder communication
8. Understand CERT-In mandatory reporting timelines and Indian regulatory requirements

Real-World Application

Incident response is a critical capability for every organization operating in the digital space. In India, CERT-In (Indian Computer Emergency Response Team) mandates that all organizations report cybersecurity incidents within **6 hours** of detection — one of the strictest timelines globally. The **Cosmos Bank heist (2018)**, where attackers siphoned INR 94 crore through

malware and SWIFT fraud, exposed gaps in incident detection and response. The **AIIMS ransomware attack (2022)**, which crippled hospital operations for over two weeks, demonstrated the devastating impact of inadequate incident response preparedness. Organizations such as **NPCI**, **HDFC Bank**, and **Infosys** maintain dedicated Security Operations Centres (SOCs) with documented playbooks for every category of cyber threat.

Hands-On Procedure

Ethical Use Disclaimer: The incident response simulations in this lab are **entirely fictional** and designed for educational purposes. All scenarios, alerts, and evidence items are simulated within the tool and do **not** interact with any real systems, networks, or data. The scenarios reference realistic attack patterns to help you understand incident response procedures. By proceeding, you agree to use the knowledge gained responsibly and in accordance with the Information Technology Act, 2000 and applicable regulations.

Part A: Environment Setup

Step 1: Clone the Incident Response Playbook Repository

Objective: Download and explore the incident response simulation project structure.
Instructions:

1. Open your terminal (bash on Linux/Mac, PowerShell on Windows)
2. Navigate to your working directory
3. Clone the repository from the provided URL
4. Navigate into the project directory
5. Explore the project structure

Code/Command:

```
# Clone the repository
git clone <repository-url> incident-response-playbook
cd incident-response-playbook

# View the top-level project structure
ls -la
# Expected directories: src/, playbooks/, templates/

# Explore the source code directory
ls src/
# Expected files:
#   models.py           - Data models for incidents, evidence, actions
#   simulator.py        - Core incident simulation engine
#   timeline.py         - Incident timeline tracker
#   severity_calculator.py - CVSS-based severity scoring
#   evidence_tracker.py - Evidence chain-of-custody manager
#   reporter.py         - Report generation engine
#   cli.py              - Command-line interface (Click-based)

# Explore the scenario files
```

```
ls src/scenarios/
# Expected files:
#   data_breach.py       - Data breach incident scenario
#   ransomware.py        - Ransomware attack scenario
#   phishing_campaign.py - Phishing campaign scenario
#   ddos_attack.py       - DDoS attack scenario
#   insider_threat.py    - Insider threat scenario

# Explore the playbooks directory
ls playbooks/
# Expected files:
#   data_breach_playbook.md
#   ransomware_playbook.md
#   phishing_campaign_playbook.md
#   ddos_attack_playbook.md
#   insider_threat_playbook.md

# Explore the templates directory
ls templates/
# Expected: HTML report templates (Jinja2)
```

Clone and Explore the Repository

Expected Output

Project directory contains:
`src/` – Core source code (models, simulator, CLI, scenarios)
`src/scenarios/` – Five Python scenario files for simulation
`playbooks/` – Five Markdown incident response playbooks
`templates/` – Jinja2 HTML report templates
`requirements.txt` – Python dependencies
`README.md` – Project overview and usage instructions

Take time to read through the project structure. Each scenario file in `src/scenarios/` defines the alerts, evidence items, decision points, and scoring criteria for a specific incident type.

Step 2: Create Virtual Environment, Install Dependencies, and Verify CLI

Objective: Set up an isolated Python environment, install required packages, and verify the CLI tool works.
Instructions:

1. Create a Python virtual environment
2. Activate the virtual environment
3. Install project dependencies from `requirements.txt`
4. Verify the CLI by testing three key commands

Code/Command:

```
# Create virtual environment
python -m venv venv

# Activate (Linux/Mac)
source venv/bin/activate

# Activate (Windows PowerShell)
.\venv\Scripts\Activate.ps1

# Install dependencies
pip install -r requirements.txt
# Installs: click, rich, jinja2, pyyaml, and other dependencies

# Verify CLI -- show available commands
python src/cli.py --help

# Verify: list available incident scenarios
python src/cli.py list-scenarios

# Verify: simulate command help
python src/cli.py simulate --help

# Verify: report generation command help
python src/cli.py generate-report --help
```

Python Environment Setup

Expected Output

CLI help output shows available commands:

```
Usage:  cli.py [OPTIONS] COMMAND [ARGS]...

Commands:
list-scenarios    List all available incident scenarios
simulate          Run an interactive incident simulation
generate-report   Generate an incident report from simulation
```

Scenario list output:

```
Available Incident Scenarios:
1.  data_breach         - Data Breach Incident
2.  ransomware          - Ransomware Attack
3.  phishing_campaign   - Phishing Campaign
4.  ddos_attack         - DDoS Attack
5.  insider_threat      - Insider Threat
```

If installation fails: (1) Ensure Python 3.8+ is installed: `python -version`, (2) Upgrade pip: `python -m pip install -upgrade pip`, (3) On Windows, ensure Python is in your PATH, (4) Try: `python -m pip install click rich jinja2` individually.

Part B: Review Incident Response Playbooks

Step 3: Review the Five Incident Response Playbooks

Objective: Read and understand the structured incident response playbooks for each threat category.
Instructions:

1. Read each of the five playbooks in the `playbooks/` directory
2. Identify the common structure across all playbooks
3. Note the specific indicators, containment steps, and recovery procedures for each incident type

Code/Command:

```
# Review the Data Breach playbook
cat playbooks/data_breach_playbook.md
# Sections: Detection Indicators, Containment Steps,
#   Eradication Procedures, Recovery Steps, Lessons Learned

# Review the Ransomware playbook
cat playbooks/ransomware_playbook.md
# Covers: File encryption detection, network isolation,
#   ransom negotiation decision tree, backup restoration

# Review the Phishing Campaign playbook
cat playbooks/phishing_campaign_playbook.md
# Covers: Email header analysis, URL reputation checking,
#   credential reset procedures, user awareness response

# Review the DDoS Attack playbook
cat playbooks/ddos_attack_playbook.md
# Covers: Traffic anomaly detection, upstream filtering,
#   CDN activation, ISP coordination, service restoration

# Review the Insider Threat playbook
cat playbooks/insider_threat_playbook.md
# Covers: Behavioral indicators, access log analysis,
#   DLP alert correlation, HR coordination, legal holds
```

Review Incident Response Playbooks

Expected Output

Each playbook follows a consistent structure:

1. Detection Indicators:
- Specific alerts, log entries, and anomalies to watch for
- Automated detection rules and manual observation cues

2. Containment Steps:
- Immediate short-term containment actions
- Long-term containment strategies
- Communication and escalation procedures

3. Eradication Procedures:
- Root cause identification steps
- Malware removal / access revocation procedures
- System hardening actions

4. Recovery Steps:
- System restoration from clean backups
- Validation and monitoring procedures
- Return to normal operations checklist

5. Lessons Learned Template:
- Post-incident review questions
- Process improvement recommendations
- Documentation and metrics tracking

Pay close attention to the **Detection Indicators** section of each playbook. In a real incident, the speed and accuracy of detection directly determines the effectiveness of the entire response. CERT-In's 6-hour reporting window begins from the moment of detection, making early identification critical.

Step 4: Map Playbook Sections to the NIST IR Lifecycle

Objective: Understand the NIST SP 800-61 Rev 2 Incident Response lifecycle and map each playbook section to its corresponding phase.
Instructions:

1. Study the four phases of the NIST IR lifecycle
2. Map each playbook section to the corresponding NIST phase
3. Understand how the phases form a continuous cycle

NIST IR Lifecycle Mapping:

Phase	NIST Phase Name	Playbook Section Mapping
1	Preparation	Organization readiness, tools, training, playbook creation itself
2	Detection & Analysis	Detection Indicators section — identifying alerts, analyzing logs, confirming the incident
3	Containment, Eradication & Recovery	Containment Steps + Eradication Procedures + Recovery Steps
4	Post-Incident Activity	Lessons Learned Template — review, documentation, process improvement

```
# The NIST IR lifecycle is cyclical, not linear:
#
# Phase 1: PREPARATION
#   - Developing IR policies and procedures
#   - Creating and maintaining playbooks (what we are reviewing)
#   - Training the IR team
#   - Deploying detection tools (SIEM, IDS/IPS, EDR)
#   - Establishing communication channels
#
# Phase 2: DETECTION & ANALYSIS
#   - Monitoring alerts from security tools
#   - Analyzing indicators of compromise (IoCs)
#   - Correlating events across multiple sources
#   - Determining incident scope and impact
#   - Classifying incident severity
#
# Phase 3: CONTAINMENT, ERADICATION & RECOVERY
#   - Short-term containment (isolate affected systems)
#   - Long-term containment (apply temporary fixes)
#   - Eradicate root cause (remove malware, patch vulns)
#   - Recover systems (restore from backups, rebuild)
#   - Validate recovery (test systems before going live)
#
# Phase 4: POST-INCIDENT ACTIVITY
#   - Conduct lessons-learned meeting
#   - Document incident timeline and decisions
#   - Update playbooks based on findings
#   - Improve detection and prevention capabilities
#   - Share threat intelligence (with CERT-In if required)
```

Understanding the NIST Mapping

The NIST lifecycle is **iterative**. During containment, you may discover new evidence that sends you back to the Detection & Analysis phase. Similarly, lessons learned from Post-Incident Activity feed directly back into improved Preparation for future incidents.

Screenshot 1

What to paste: Terminal output showing the project directory structure (`ls` of the repo root, `src/`, `src/scenarios/`, and `playbooks/` directories) alongside the output of `python src/cli.py list-scenarios` showing all five available scenarios.

Paste your screenshot here

Part C: Incident Simulation

Step 5: Simulate a Data Breach Incident

Objective: Run an interactive data breach simulation, respond to alerts, choose response actions, and receive a performance score.
Instructions:

1. List available scenarios to confirm readiness
2. Launch the data breach simulation
3. Read each alert and evidence item carefully
4. Choose response actions at each decision point
5. Review your performance score at the end

Code/Command:

```
# First, list all available scenarios
python src/cli.py list-scenarios

# Launch the data breach simulation
python src/cli.py simulate --scenario data_breach

# The simulation presents a series of phases:
#
# PHASE 1 - DETECTION:
#   Alert: Unusual database query volume detected
#   Alert: Large data export from customer records table
#   Alert: Unrecognized IP accessing admin panel
#   -> Choose: Investigate immediately / Escalate / Ignore
#
# PHASE 2 - ANALYSIS:
#   Evidence: Access logs show brute-force on admin login
#   Evidence: SQL injection payload found in web logs
#   Evidence: 50,000 customer records accessed in 2 hours
#   -> Choose: Classify as incident / Continue monitoring
#
# PHASE 3 - CONTAINMENT:
#   -> Choose: Block attacker IP / Disable admin account /
#              Take database offline / All of the above
#
# PHASE 4 - ERADICATION:
#   -> Choose: Patch SQL injection / Reset all passwords /
#              Deploy WAF / Review access controls
#
# PHASE 5 - RECOVERY:
#   -> Choose: Restore from backup / Rebuild from scratch /
#              Validate data integrity / Notify stakeholders
#
# PHASE 6 - POST-INCIDENT:
#   -> Choose actions for lessons learned documentation
```

Data Breach Simulation

Expected Output

Simulation output (interactive):

```
================================================
INCIDENT SIMULATION: Data Breach
================================================
[ALERT] Unusual database query volume detected
[ALERT] Large data export from customer records
[ALERT] Unrecognized IP: 203.0.113.42

What is your first response action?
1.  Investigate immediately
2.  Escalate to IR team lead
3.  Continue monitoring
4.  Ignore - likely false positive
> Your choice:  1

[CORRECT] Good - immediate investigation is critical
Points:  +10

...additional phases follow...

================================================
SIMULATION COMPLETE
Your Score:  78/100
Rating:  Competent Responder
Areas for Improvement:
- Consider notifying CERT-In within 6 hours
- Evidence preservation should happen earlier
================================================
```

The simulation scores your responses based on incident response best practices. There is no single "correct" path — the tool evaluates the **appropriateness and timeliness** of your actions. Prioritizing containment over investigation, or skipping stakeholder notification, will reduce your score.

Screenshot 2

What to paste: Terminal output showing the data breach simulation in progress, including at least one alert display and one interactive decision point where you are choosing a response action, along with the scoring feedback.

Paste your screenshot here

Step 6: Simulate a Ransomware Attack

Objective: Run a ransomware attack simulation with critical decision points including the ransom payment dilemma, containment strategy, backup restoration, and communication planning.

Instructions:

1. Launch the ransomware simulation
2. Face the ransom payment decision — evaluate the trade-offs
3. Choose containment and network isolation strategies
4. Decide on backup restoration approach
5. Plan stakeholder and media communications
6. Review your final performance score

Code/Command:

```
# Launch the ransomware simulation
python src/cli.py simulate --scenario ransomware

# Key decision points in the ransomware scenario:
#
# DETECTION PHASE:
#   Alert: File encryption activity detected on file server
#   Alert: Ransom note found on encrypted systems
#   Alert: Multiple endpoint AV alerts for known ransomware
#   -> Choose detection response
#
# CONTAINMENT DECISION:
#   -> Isolate affected systems from network?
#   -> Shut down file sharing services?
#   -> Disable VPN access for remote users?
#   -> Preserve forensic evidence before containment?
#
# RANSOM PAYMENT DECISION:
#   Ransom demand: 50 BTC (~INR 20 crore)
#   -> Pay ransom (risk: no guarantee of decryption)
#   -> Refuse and restore from backups
#   -> Negotiate with attackers
#   -> Contact law enforcement (CERT-In, Cyber Crime Cell)
#
# BACKUP RESTORATION:
#   -> Full restore from last clean backup
#   -> Partial restore (critical systems first)
#   -> Rebuild affected systems from scratch
#   -> Verify backup integrity before restoration
#
# COMMUNICATION PLAN:
#   -> Internal: CEO, Board, IT team, all employees
#   -> External: CERT-In (mandatory), customers, media
#   -> Legal: Data Protection Officer, legal counsel
#   -> Regulatory: RBI (if financial institution)
```

Ransomware Attack Simulation

Expected Output

Ransomware simulation output:

```
================================================
INCIDENT SIMULATION: Ransomware Attack
================================================
[CRITICAL ALERT] Ransomware detected!
[EVIDENCE] 2,847 files encrypted (.locked extension)
[EVIDENCE] Ransom note:  DECRYPT_FILES.txt
[EVIDENCE] Lateral movement detected via SMB

CRITICAL DECISION: Pay the ransom?
1.  Pay ransom (50 BTC)
2.  Refuse - restore from backups
3.  Negotiate for lower amount
4.  Contact law enforcement first
> Your choice:  2

[RECOMMENDED] Refusing ransom is best practice.
FBI, CERT-In, and NCSC advise against payment.
Points:  +15

...additional decision points...

================================================
SIMULATION COMPLETE
Your Score:  85/100
Rating:  Skilled Responder
Key Strengths:
- Correct decision on ransom payment
- Timely network isolation
Areas for Improvement:
- Verify backup integrity before restoring
================================================
```

CERT-In, FBI, Europol, and the UK NCSC all recommend **against paying ransoms**. Payment does not guarantee data recovery, funds criminal operations, and marks the victim as a future target. The **AIIMS ransomware attack (2022)** was resolved without paying ransom by rebuilding systems from backups over approximately two weeks.

Screenshot 3

What to paste: Terminal output showing the ransomware simulation with the ransom payment decision point visible, your chosen response, and the scoring feedback showing your performance rating.

Paste your screenshot here

Step 7: Review Incident Timeline and Evidence Tracker

Objective: Examine the incident timeline generated during simulation and review the evidence items with chain-of-custody metadata.
Instructions:

1. After completing a simulation, review the auto-generated incident timeline
2. Examine timestamp entries for every alert, action, and decision made
3. Review evidence items collected during the simulation
4. Understand chain-of-custody metadata (who collected, when, storage location, integrity hash)

Code/Command:

```
# The simulation automatically generates a timeline
# Review it after the simulation completes

# The timeline includes auto-generated timestamps:
#   T+00:00  - Initial alert received
#   T+00:05  - Analyst begins investigation
#   T+00:12  - Incident confirmed and classified
#   T+00:15  - Containment actions initiated
#   T+00:30  - IR team lead notified
#   T+01:00  - Eradication procedures started
#   T+02:30  - Recovery operations begin
#   T+04:00  - Systems validated and returned to service
#   T+05:30  - CERT-In notification submitted
#   T+06:00  - Post-incident review scheduled

# Evidence items tracked during simulation include:
#   - Network access logs (source IPs, timestamps)
#   - Database query logs (unusual queries, data volumes)
#   - Malware samples (file hashes, signatures)
#   - System memory dumps (volatile data)
#   - Disk images (forensic copies)
#   - Email headers (phishing artifacts)
#   - Screenshots (ransom notes, alerts)

# Each evidence item includes chain-of-custody metadata:
#   - Evidence ID (unique identifier)
#   - Description (what was collected)
#   - Collected By (analyst name/role)
#   - Collection Time (timestamp)
#   - Storage Location (evidence locker/server)
#   - Integrity Hash (SHA-256 hash for verification)
#   - Chain of Custody Log (transfers and access)
```

Review Timeline and Evidence

Expected Output

Incident Timeline:

```
================================================
INCIDENT TIMELINE: Data Breach
================================================
T+00:00  [DETECT]  Unusual DB query volume alert
T+00:03  [DETECT]  Large data export flagged
T+00:05  [ACTION]  Analyst begins investigation
T+00:12  [DECIDE]  Classified as security incident
T+00:15  [ACTION]  Attacker IP blocked at firewall
T+00:18  [ACTION]  Admin account disabled
T+00:25  [ESCAL]  IR team lead notified
T+01:00  [ACTION]  SQL injection patched
T+02:30  [ACTION]  Systems restored from backup
T+05:00  [NOTIFY]  CERT-In report submitted
================================================
```

Evidence Tracker:

```
================================================
EVIDENCE LOG
================================================
EVD-001:  Web server access logs
Collected:  T+00:08 by SOC Analyst
Hash:  sha256:a1b2c3d4e5f6...
Storage:  Evidence Server /cases/2024-001/
EVD-002:  Database query logs
Collected:  T+00:10 by DBA
Hash:  sha256:f6e5d4c3b2a1...
EVD-003:  Firewall logs (attacker IP)
Collected:  T+00:20 by Network Admin
Hash:  sha256:1a2b3c4d5e6f...
================================================
```

Proper evidence handling is essential for both forensic investigation and legal proceedings. In India, digital evidence must comply with the Indian Evidence Act (Section 65B) and IT Act requirements. An unbroken chain of custody with integrity hashes ensures evidence is admissible in court.

Screenshot 4

What to paste: Terminal output showing the incident timeline (with timestamps and action types) and the evidence tracker output (showing evidence IDs, descriptions, collection metadata, and integrity hashes).

Paste your screenshot here

Part D: Severity Assessment & Reporting

Step 8: Calculate Incident Severity

Objective: Use CVSS-based severity scoring to assess the impact of a simulated incident, including financial, reputational, and regulatory dimensions.
Instructions:

1. Run the data breach simulation with severity calculation enabled
2. Review the CVSS-based severity score
3. Examine business impact estimates across multiple dimensions
4. Understand the severity classification (Critical/High/Medium/Low)

Code/Command:

```
# Run simulation with severity calculation
python src/cli.py simulate \
    --scenario data_breach \
    --calculate-severity

# The severity calculator evaluates:
#
# CVSS Base Metrics:
#   - Attack Vector (Network/Adjacent/Local/Physical)
#   - Attack Complexity (Low/High)
#   - Privileges Required (None/Low/High)
#   - User Interaction (None/Required)
#   - Scope (Changed/Unchanged)
#   - Confidentiality Impact (High/Low/None)
#   - Integrity Impact (High/Low/None)
#   - Availability Impact (High/Low/None)
#
# Business Impact Assessment:
#   - Financial Loss Estimate (direct + indirect costs)
#   - Reputational Damage Score (customer trust impact)
#   - Regulatory Exposure (fines, penalties, compliance)
#   - Operational Downtime (hours of service disruption)
#
# Severity Classification:
#   Critical (9.0-10.0): Immediate executive notification
#   High (7.0-8.9): IR team mobilization within 1 hour
#   Medium (4.0-6.9): Scheduled response within 4 hours
#   Low (0.1-3.9): Standard ticket, next business day
```

Severity Calculation

Expected Output

Severity Assessment Output:

```
================================================
SEVERITY ASSESSMENT: Data Breach
================================================

CVSS Base Score:  9.1 (CRITICAL)
Attack Vector:        Network
Attack Complexity:    Low
Privileges Required:  None
User Interaction:     None
Confidentiality:      High
Integrity:            Low
Availability:         None

BUSINESS IMPACT ESTIMATE:
Financial Loss:       INR 2.5 - 5.0 Crore
(breach costs, forensics, legal, notification)
Reputational Damage:  HIGH
(customer trust erosion, media coverage)
Regulatory Exposure:  CRITICAL
(DPDP Act fine up to INR 250 Crore)
(CERT-In 6-hr reporting mandatory)
Operational Downtime: 8-24 hours

CLASSIFICATION: CRITICAL
Required Actions:
- Immediate executive notification
- CERT-In report within 6 hours
- Activate full IR team
- Engage external forensics firm
================================================
```

Under the Digital Personal Data Protection (DPDP) Act, 2023, data breach fines in India can reach up to **INR 250 Crore**. Combined with CERT-In's 6-hour mandatory reporting and RBI's separate reporting requirements for financial institutions, the regulatory exposure for data breaches in India is substantial.

Step 9: Generate Professional Incident Report

Objective: Generate a comprehensive HTML incident report from the simulation data, including executive summary, timeline, evidence log, findings, recommendations, and lessons learned.

Instructions:

1. Run the report generation command for the data breach scenario
2. Open the generated HTML report in your browser
3. Review each section of the report
4. Identify the executive summary, timeline, and recommendations

Code/Command:

```
# Generate HTML incident report
python src/cli.py generate-report \
    --scenario data_breach \
    --format html \
    --output incident_report.html

# Open the report in browser (Linux/Mac)
open incident_report.html

# Open the report in browser (Windows)
start incident_report.html

# The report contains the following sections:
#
# 1. EXECUTIVE SUMMARY
#    - Incident type, severity, and classification
#    - Timeline summary (detection to resolution)
#    - Business impact overview
#    - Key findings and recommended actions
#
# 2. INCIDENT TIMELINE
#    - Chronological event log with timestamps
#    - Actions taken at each phase
#    - Decisions made and their rationale
#
# 3. EVIDENCE LOG
#    - All evidence items with chain-of-custody
#    - Integrity hashes and storage locations
#    - Collection methodology
#
# 4. FINDINGS
#    - Root cause analysis
#    - Attack vector identification
#    - Scope of compromise
#    - Data affected (volume, type, sensitivity)
#
# 5. RECOMMENDATIONS
#    - Immediate remediation actions
#    - Short-term security improvements
#    - Long-term strategic recommendations
#    - Compliance actions (CERT-In, DPDP Act)
#
# 6. LESSONS LEARNED
#    - What went well during the response
#    - What could be improved
#    - Process and playbook updates needed
#    - Training recommendations
```

Generate Incident Report

Expected Output

Report generation output:

```
================================================
REPORT GENERATION
================================================
Scenario:  Data Breach
Format:  HTML
Template:  templates/incident_report.html.j2
Output:  incident_report.html

Report sections generated:
[OK] Executive Summary
[OK] Incident Timeline (12 entries)
[OK] Evidence Log (5 items)
[OK] Findings (3 root causes)
[OK] Recommendations (8 actions)
[OK] Lessons Learned (6 items)

Report generated successfully!
File:  incident_report.html (42 KB)
================================================
```

In practice, incident reports are shared with executive leadership, legal counsel, and regulators. The report must be factual, precise, and avoid speculation. Under CERT-In's 2022 directive, the incident report must include: nature of the incident, systems affected, impact assessment, and remedial actions taken.

Screenshot 5

What to paste: The HTML incident report (`incident_report.html`) opened in your web browser, showing the executive summary section (incident type, severity, business impact) and the beginning of the incident timeline section.

Paste your screenshot here

Conceptual Background

NIST SP 800-61 Rev 2: Incident Response Lifecycle

The National Institute of Standards and Technology (NIST) Special Publication 800-61 Revision 2, "Computer Security Incident Handling Guide," defines the authoritative framework for incident response. The lifecycle consists of four interconnected phases:

Phase 1: Preparation

Preparation is the foundation of effective incident response. It involves:

- **Policy and Procedures:** Developing and maintaining an incident response policy, plan, and procedures tailored to the organization's risk profile.
- **Incident Response Team:** Establishing a Computer Security Incident Response Team (CSIRT) with defined roles — IR Manager, Lead Analyst, Forensic Specialist, Communications Lead.
- **Tools and Infrastructure:** Deploying SIEM systems, intrusion detection/prevention systems (IDS/IPS), endpoint detection and response (EDR) tools, forensic workstations, and secure communication channels.
- **Playbooks:** Creating detailed, step-by-step playbooks for common incident types (as explored in this practical).
- **Training and Exercises:** Regular tabletop exercises, red team/blue team drills, and awareness training.
- **Communication Plans:** Pre-defined escalation paths, stakeholder notification templates, and media response guidelines.

Phase 2: Detection and Analysis

This phase involves identifying that a security event has occurred and determining its nature and scope:

- **Detection Sources:** Security alerts from SIEM, IDS/IPS, antivirus, EDR, user reports, threat intelligence feeds, law enforcement notifications.
- **Indicators of Compromise (IoCs):** Specific artifacts that indicate malicious activity — suspicious IP addresses, file hashes, unusual network traffic patterns, registry changes.
- **Triage and Classification:** Determining whether an event is a true security incident, classifying its type and severity, and prioritizing the response.

- **Scope Determination:** Identifying which systems, data, and users are affected, and whether the attack is still active or has been contained.
- **Documentation:** Maintaining a detailed timeline from the first alert through analysis, recording all observations and decisions.

Phase 3: Containment, Eradication, and Recovery

This is the action phase where the incident is stopped and damage is repaired:

- **Short-Term Containment:** Immediate actions to stop the attack from spreading — network isolation, account disabling, firewall rules. The goal is to limit damage while preserving evidence.
- **Long-Term Containment:** Temporary fixes that allow business to continue while a permanent solution is developed — applying patches, deploying additional monitoring, rerouting traffic.
- **Eradication:** Removing the root cause — malware removal, vulnerability patching, closing unauthorized access paths, resetting compromised credentials.
- **Recovery:** Restoring systems to normal operation — rebuilding from clean images, restoring from verified backups, validating system integrity, monitoring for re-infection.

Phase 4: Post-Incident Activity

The final phase ensures continuous improvement:

- **Lessons Learned Meeting:** Formal review within 1–2 weeks of incident closure, involving all stakeholders. Key questions: What happened? What went well? What could be improved?
- **Incident Documentation:** Complete incident report with timeline, evidence, decisions, outcomes, and metrics (time to detect, time to contain, time to recover).
- **Playbook Updates:** Revising and improving playbooks based on the actual incident experience.
- **Threat Intelligence Sharing:** Sharing IoCs, attack patterns, and TTPs with CERT-In, industry ISACs, and partner organizations.
- **Metrics and Reporting:** Tracking KPIs such as Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), and Mean Time to Recover (MTTR).

Incident Classification

Security Events vs. Security Incidents

- **Security Event:** Any observable occurrence in a system or network — a login attempt, a firewall log entry, a port scan. Most security events are benign.
- **Security Incident:** A security event that actually violates the organization's security policy or poses a genuine threat — successful unauthorized access, malware infection, data exfiltration, service disruption.
- Not every event becomes an incident. The Detection and Analysis phase determines whether an event meets the threshold for incident classification.

Severity Levels

Level	CVSS Range	Characteristics
Critical	9.0–10.0	Active data exfiltration, complete system compromise, widespread ransomware, critical infrastructure affected
High	7.0–8.9	Significant data exposure, partial system compromise, active attack requiring immediate containment
Medium	4.0–6.9	Limited data exposure, vulnerability being actively probed, contained but requiring remediation
Low	0.1–3.9	Policy violation, reconnaissance activity, unsuccessful attack attempt, informational findings

Common Incident Types

- **Data Breach:** Unauthorized access to or exfiltration of sensitive data — customer records, financial data, intellectual property, personal health information.
- **Ransomware:** Malware that encrypts files and demands payment for decryption keys. Often accompanied by data exfiltration (double extortion).
- **Phishing Campaign:** Targeted or mass emails designed to steal credentials, deliver malware, or manipulate users into financial transfers (BEC fraud).
- **DDoS Attack:** Distributed Denial of Service — overwhelming a target's infrastructure with traffic to cause service outage.
- **Insider Threat:** Malicious or negligent actions by employees, contractors, or trusted partners — data theft, sabotage, policy violations.
- **Supply Chain Attack:** Compromise through a trusted third-party vendor, software library, or update mechanism (e.g., SolarWinds, Log4j).

Evidence Handling and Digital Forensics

Chain of Custody

Chain of custody is the documented, unbroken trail showing the collection, transfer, and handling of evidence:

- **Collection:** Document who collected the evidence, when, where, and how.
- **Preservation:** Create forensic copies (bit-for-bit images), compute integrity hashes (SHA-256), and store originals securely.
- **Transfer:** Record every transfer of evidence between individuals, with timestamps and signatures.
- **Analysis:** Work only on forensic copies, never on originals. Document all analysis tools and methods used.
- **Storage:** Maintain evidence in a secure, access-controlled location with environmental controls.

Volatile Data Collection Order

Digital evidence must be collected in order of volatility (most volatile first):

1. **CPU Registers and Cache:** Most volatile, lost immediately when power is removed
2. **System Memory (RAM):** Running processes, network connections, encryption keys
3. **Network State:** Active connections, routing tables, ARP cache
4. **Running Processes:** Process list, open files, loaded modules
5. **Disk Data:** File systems, swap space, temporary files
6. **Log Files:** System, application, and security logs
7. **Archival Media:** Backups, external storage, cloud snapshots

Log Preservation

Critical logs to preserve during an incident:

- **System Logs:** Windows Event Logs, Linux syslog/journald, authentication logs
- **Application Logs:** Web server access/error logs, database query logs, application-specific logs
- **Network Logs:** Firewall logs, IDS/IPS alerts, DNS query logs, proxy logs, NetFlow data

- **Security Tool Logs:** SIEM alerts, EDR telemetry, antivirus detection logs, DLP alerts
- **Cloud Logs:** AWS CloudTrail, Azure Activity Log, GCP Cloud Audit Logs

Incident Communication

Stakeholder Notification

Different stakeholders require different levels of detail and urgency:

Stakeholder	Timing	Content
IR Team	Immediately	Full technical details, IoCs, containment instructions
Executive/Board	Within 1 hour	Business impact summary, risk assessment, recommended actions
Legal Counsel	Within 2 hours	Regulatory obligations, liability assessment, evidence preservation
Regulators (CERT-In)	Within 6 hours	Incident type, affected systems, impact, remedial actions
Affected Customers	As required	Clear notification, what data was affected, protective actions
Media/Public	After legal review	Prepared statement, key facts, remediation steps taken

Media Handling

- Designate a single spokesperson — typically the Communications Lead or CISO
- Prepare holding statements in advance as part of IR planning
- Be transparent but do not speculate or share unverified details
- Coordinate with legal counsel before any public statement
- Provide regular updates as the investigation progresses

Business Impact Analysis

Every incident carries multiple dimensions of business impact:

- **Financial Loss:** Direct costs (forensics, legal fees, notification, credit monitoring, regulatory fines) plus indirect costs (lost revenue during downtime, increased insurance premiums, emergency vendor contracts).

- **Operational Downtime:** Service unavailability, reduced productivity, manual workarounds, delayed customer deliverables.
- **Reputational Damage:** Customer trust erosion, media coverage, social media backlash, loss of competitive advantage, difficulty attracting talent.
- **Regulatory Fines:** DPDP Act fines up to INR 250 Crore, RBI penalties for non-compliance, CERT-In enforcement actions, GDPR fines for cross-border incidents (up to 4% of global turnover).

India-Specific Incident Reporting Requirements

CERT-In Mandatory Incident Reporting

The Indian Computer Emergency Response Team (CERT-In), established under the IT Act 2000 Section 70B, issued directives in April 2022 that mandate:

- **6-Hour Reporting Requirement:** All organizations must report cybersecurity incidents to CERT-In within **6 hours** of noticing or being notified of the incident. This is among the strictest timelines in the world (EU NIS2 requires 24 hours; US CIRCIA requires 72 hours).
- **Reportable Incident Types:** Targeted scanning/probing of critical systems, compromise of critical systems, unauthorized access, website defacement, malware attacks, identity theft/phishing, DDoS attacks, data breaches, attacks on critical infrastructure, attacks on IoT/OT devices, and fake mobile apps.
- **Log Retention:** All service providers, intermediaries, data centres, and government bodies must maintain logs of all ICT systems for a rolling period of **180 days** within Indian jurisdiction.
- **Synchronization:** All ICT system clocks must be synchronized with the National Physical Laboratory (NPL) or the National Informatics Centre (NIC) Network Time Protocol (NTP) servers.
- **Reporting Format:** Incidents must be reported via email (`incident@cert-in.org.in`), phone, or fax in the prescribed format including: incident type, affected systems, geographic location, IP addresses, time of occurrence, and remedial actions.
- **Non-Compliance Penalties:** Failure to report carries penalties under IT Act Section 70B(7) — imprisonment up to one year and/or fine up to INR 1 Lakh.

RBI Cyber Incident Reporting for Banks

The Reserve Bank of India mandates additional requirements for banks and financial institutions:

- **Immediate Reporting:** Banks must report cybersecurity incidents to the RBI CSITE (Cyber Security and IT Examination) cell immediately upon detection.

- **Detailed Report:** A comprehensive incident report must be submitted within 24–48 hours, including root cause analysis, scope of impact, and remediation plan.
- **Board Reporting:** The Board of Directors must be informed of significant cyber incidents, and the Chief Information Security Officer (CISO) must present a quarterly security review.
- **Customer Notification:** Customers whose data or accounts are affected must be notified promptly and guided on protective measures (password reset, card blocking, transaction monitoring).
- **VAPT and SOC:** Banks must maintain 24x7 Security Operations Centres and conduct Vulnerability Assessment and Penetration Testing at least quarterly.
- **Cyber Crisis Management Plan (CCMP):** Banks must maintain and regularly test a CCMP that covers detection, response, recovery, and communication for cyber incidents.

IT Act 2000 – Section 70B: CERT-In Powers

Section 70B of the Information Technology Act, 2000, empowers CERT-In as the national agency for incident response:

- Serve as the national point of contact for computer security incidents
- Collect, analyze, and disseminate information on cyber incidents
- Issue forecasts and alerts regarding cybersecurity incidents
- Provide emergency measures for handling cybersecurity incidents
- Coordinate cyber incident response activities
- Issue guidelines, advisories, and vulnerability notes
- Perform and commission functions relating to cybersecurity

DPDP Act 2023 – Breach Notification

The Digital Personal Data Protection Act, 2023, introduces specific requirements:

- **72-Hour Notification:** Data Fiduciaries (controllers) must notify the Data Protection Board (DPB) and affected Data Principals (individuals) of any personal data breach within **72 hours** of becoming aware.
- **Content:** Notification must include the nature of the breach, categories of data affected, approximate number of individuals affected, potential consequences, and measures taken to mitigate.
- **Penalties:** Non-compliance can result in fines up to INR 250 Crore per instance, as determined by the Data Protection Board.

- **Significant Data Fiduciary:** Organizations classified as Significant Data Fiduciaries face enhanced obligations including mandatory Data Protection Impact Assessments and periodic audits.

Notable Indian Cyber Incidents

Cosmos Bank Heist (2018)

- **What happened:** Attackers compromised the bank's ATM switch server (Flexcube), installed malware, and cloned thousands of debit card details. Over a weekend, simultaneous withdrawals were made from ATMs across 28 countries. Separately, three fraudulent SWIFT transfers were initiated to a Hong Kong account.
- **Impact:** Total loss of approximately INR 94.42 Crore (USD 13.5 million).
- **Response:** The bank isolated its ATM server, notified RBI and CERT-In, engaged forensic investigators, and worked with international law enforcement. Recovery took months.
- **Lessons:** Need for network segmentation, real-time transaction monitoring, and independent SWIFT validation. Highlighted gaps in weekend/holiday monitoring.

Juspay Data Breach (2020)

- **What happened:** Juspay, a payment gateway processing transactions for Amazon, Flipkart, and other major platforms, suffered a server breach. Masked card numbers and email addresses of approximately 10 crore users were exfiltrated.
- **Impact:** Massive reputational damage, customer data exposed on dark web, regulatory scrutiny.
- **Response:** Juspay issued a public statement, notified affected merchants, conducted forensic investigation, implemented additional security controls, and engaged with CERT-In.
- **Lessons:** Importance of data minimization, encryption at rest, server hardening, and proactive breach detection. Exposed the interconnected risk in India's fintech ecosystem.

AIIMS Ransomware Attack (2022)

- **What happened:** The All India Institute of Medical Sciences (AIIMS), New Delhi, was hit by a ransomware attack that encrypted approximately 1.3 TB of data across five servers. The attack disrupted patient registration, admissions, billing, laboratory, and reporting systems for over two weeks.
- **Impact:** Hospital operations reverted to manual processes. An estimated 3–4 crore patient records were potentially compromised, including those of VVIPs.

- **Response:** CERT-In, NIA, Delhi Police Cyber Cell, and DRDO collaborated on the response. Systems were rebuilt from scratch over approximately 15 days. The ransom (reportedly INR 200 Crore in cryptocurrency) was **not paid**.
- **Lessons:** Critical need for backup strategies in healthcare, network segmentation, endpoint protection, and cybersecurity investment in public sector institutions. Led to increased government focus on protecting Critical Information Infrastructure (CII).

Assessment & Deliverables

Assessment Questions

Answer the following questions in your submission:

Q1. Describe the four phases of the NIST SP 800-61 Rev 2 Incident Response lifecycle. For each phase, explain its purpose and provide one specific activity that takes place during that phase.

Q2. Explain how CVSS-based severity scoring works for incident classification. What factors distinguish a Critical-severity incident from a High-severity incident? Provide an example scenario for each.

Q3. Describe the importance of evidence chain-of-custody in incident response. What five elements must be documented for each evidence item? Why is the order of volatile data collection important?

Q4. Explain CERT-In's mandatory 6-hour incident reporting requirement. What types of incidents must be reported? What are the penalties for non-compliance? How does this compare to international timelines (EU NIS2, US CIRCIA)?

Q5. What communication steps should be taken when a data breach is confirmed? List at least five different stakeholder groups and explain what information each group needs and when they should be notified.

Q6. Analyze the AIIMS ransomware attack (2022). What was the attack? How was it handled? Was the ransom paid? What lessons can organizations learn about ransomware preparedness?

Q7. Explain the difference between a security event and a security incident. Provide three examples of events that would be classified as incidents and three that would not.

Q8. Describe the requirements of the DPDP Act 2023 regarding data breach notification. What is the notification timeline? Who must be notified? What are the maximum penalties for non-compliance?

Deliverables Checklist

Item	Description	Type	Status
Screenshot 1	Repo structure + scenarios list	Paste	☐
Screenshot 2	Data breach simulation decision	Paste	☐
Screenshot 3	Ransomware simulation + scoring	Paste	☐
Screenshot 4	Timeline + evidence tracker	Paste	☐
Screenshot 5	HTML incident report	Paste	☐
Answers	Q1–Q8 written responses	Text	☐
Report File	Generated `incident_report.html`	File	☐
Sim Scores	Simulation scores for both scenarios	Text	☐

Verification Checklist

Complete all items below before submitting:

- ☐ Repository cloned and virtual environment set up
- ☐ CLI verified with `list-scenarios`, `simulate -help`, and `generate-report -help`
- ☐ All five playbooks reviewed (data breach, ransomware, phishing, DDoS, insider threat)
- ☐ NIST IR lifecycle phases mapped to playbook sections
- ☐ Data breach simulation completed with response scoring
- ☐ Ransomware simulation completed including ransom payment decision
- ☐ Incident timeline reviewed with timestamp entries
- ☐ Evidence tracker reviewed with chain-of-custody metadata
- ☐ Severity calculation completed with CVSS score and business impact
- ☐ HTML incident report generated and opened in browser
- ☐ All 5 required screenshots captured and pasted
- ☐ All 8 assessment questions answered

Grading Rubric

Criteria	Description	Points	Score
Setup	Repo cloned, environment ready, CLI verified	10	___/10
Playbook Review	Five playbooks reviewed, NIST mapping completed	10	___/10
Data Breach Sim	Simulation completed with scoring	15	___/15
Ransomware Sim	Simulation completed with ransom decision	15	___/15
Timeline/Evidence	Timeline and evidence tracker reviewed	10	___/10
Severity Calc	CVSS scoring and business impact assessed	10	___/10
Report Generation	HTML report generated and analyzed	10	___/10
Assessment	Q1–Q8 answered correctly	10	___/10
Screenshots	All 5 screenshots captured and pasted	10	___/10
	TOTAL	**100**	___/100

Appendix A: NIST IR Lifecycle Summary Table

Phase	Name	Key Activities	Key Outputs
1	Preparation	Policy development, team training, tool deployment, playbook creation, exercises	IR Plan, playbooks, trained team, communication plan
2	Detection & Analysis	Alert monitoring, event correlation, triage, scope determination, severity classification	Incident classification, scope assessment, initial timeline
3	Containment, Eradication & Recovery	System isolation, malware removal, vulnerability patching, backup restoration, validation	Contained threat, clean systems, restored operations
4	Post-Incident Activity	Lessons learned meeting, documentation, playbook updates, metrics tracking, intel sharing	Incident report, updated playbooks, improved processes

Appendix B: Severity Scoring Matrix

Severity	CVSS	Examples	Response Time	Escalation
Critical	9.0–10.0	Active data exfiltration, ransomware spreading, CII compromise	Immediate (15 min)	CISO, CEO, Board
High	7.0–8.9	Confirmed unauthorized access, significant data exposure	Within 1 hour	IR Manager, CISO
Medium	4.0–6.9	Vulnerability under active probing, limited exposure	Within 4 hours	IR Team Lead
Low	0.1–3.9	Policy violation, failed attack, reconnaissance	Next business day	SOC Analyst

Appendix C: Evidence Collection Checklist

Evidence Type	Volatility	Collected	Notes
System memory (RAM) dump	Very High	☐	Use `winpmem` or `LiME`
Network connections	High	☐	`netstat -an`, packet captures
Running processes	High	☐	Process list with command lines
System/security logs	Medium	☐	Export before rotation
Web server access logs	Medium	☐	Include error logs
Database query logs	Medium	☐	Suspicious queries, timestamps
Firewall/IDS logs	Medium	☐	Rule hits, blocked connections
Disk forensic image	Low	☐	Bit-for-bit copy with hashing
Email headers/artifacts	Low	☐	Phishing emails, attachments
Malware samples	Low	☐	Isolate in sandbox, hash files
Cloud audit logs	Low	☐	CloudTrail, Activity Log
Backup verification	Low	☐	Confirm backup integrity

Appendix D: Incident Communication Template

Initial Notification Template (Internal)

SECURITY INCIDENT NOTIFICATION

Incident ID: [Auto-generated]
Classification: [Critical / High / Medium / Low]
Date/Time Detected: [DD/MM/YYYY HH:MM IST]
Reported By: [Name, Role]

Incident Type: [Data Breach / Ransomware / Phishing / DDoS / Insider Threat / Other]

Affected Systems: [List of systems, applications, services]
Affected Data: [Type and estimated volume]
Current Status: [Detected / Under Investigation / Contained / Resolved]

Immediate Actions Taken:
1. [Action 1]
2. [Action 2]
3. [Action 3]

Next Steps:
1. [Planned action 1]
2. [Planned action 2]

CERT-In Reporting Status: [Pending / Submitted / Not Required]
CERT-In Reporting Deadline: [6 hours from detection: HH:MM IST]

Customer Notification Template

Subject: Important Security Notice

Dear [Customer Name],

We are writing to inform you of a security incident that may have affected your personal data. We take the security of your information very seriously and want to provide you with the details and steps we are taking.

What Happened: [Brief, factual description]
What Data Was Involved: [Types of data, NOT specific values]
What We Are Doing: [Remediation actions taken]
What You Can Do: [Recommended protective actions]

We have reported this incident to CERT-In and the relevant regulatory authorities as required by law. We are cooperating fully with the investigation.

For questions, please contact: [Dedicated helpline/email]

Sincerely,
[Organization Name]

Appendix E: CERT-In Reporting Requirements Summary

Requirement	Details
Reporting Timeline	Within 6 hours of noticing or being notified of the incident
Reporting Channels	Email: `incident@cert-in.org.in`, Phone: 1800-11-4949, Fax
Reportable Incidents	Targeted scanning, system compromise, unauthorized access, defacement, malware, identity theft, phishing, DDoS, data breach, attacks on CII, attacks on IoT/OT, fake mobile apps
Required Information	Incident type, affected systems, geographic location, IP addresses, time of occurrence, remedial actions, organization details
Log Retention	180 days, within Indian jurisdiction
Clock Synchronization	Must sync with NPL/NIC NTP servers
Applicable To	Service providers, intermediaries, data centres, body corporates, government organizations
Non-Compliance Penalty	IT Act Section 70B(7): Imprisonment up to 1 year and/or fine up to INR 1 Lakh

Appendix F: Troubleshooting Guide

Problem: `python src/cli.py` returns `ModuleNotFoundError` or command not found
Solutions:

1. Ensure virtual environment is activated: check for `(venv)` prefix in terminal
2. Verify dependencies: `pip list | grep click` and `pip list | grep rich`
3. Reinstall dependencies: `pip install -r requirements.txt`
4. On Windows, use `python` not `python3`; on Linux/Mac, try `python3`

Problem: The interactive simulation freezes or does not accept keyboard input
Solutions:

1. Ensure you are entering a valid option number (1, 2, 3, etc.) and pressing Enter
2. Check that the Rich library is installed: `pip install rich`
3. Try running in a standard terminal (not IDE integrated terminal)
4. On Windows, try running in Windows Terminal or PowerShell instead of CMD
5. Restart the simulation: `Ctrl+C` and re-run the command

Problem: `generate-report` command fails or the HTML file is empty/malformed
Solutions:

1. Ensure a simulation has been completed before generating the report
2. Verify Jinja2 is installed: `pip install jinja2`
3. Check that `templates/` directory exists and contains `.html.j2` template files
4. Try a different output path: `-output /tmp/incident_report.html`
5. Check terminal for specific error messages and stack traces

Appendix G: Additional Resources

Official Documentation

→ NIST SP 800-61 Rev 2: `https://csrc.nist.gov/pubs/sp/800/61/r2/final`

→ CERT-In: `https://www.cert-in.org.in/`

→ CERT-In Directions (2022): `https://www.cert-in.org.in/Directions70B.jsp`

→ RBI Cyber Security Framework: `https://www.rbi.org.in`

→ DPDP Act 2023: `https://www.meity.gov.in/data-protection-framework`

→ IT Act 2000: `https://www.meity.gov.in/content/information-technology-act`

→ FIRST CVSS Calculator: `https://www.first.org/cvss/calculator/3.1`

Learning Resources

- "Incident Response & Computer Forensics" – Luttgens, Pepe, Mandia (3rd Edition)

- "The CERT Guide to Insider Threats" – Cappelli, Moore, Trzeciak
- "Blue Team Handbook: Incident Response Edition" – Don Murdoch
- "Digital Forensics with Kali Linux" – Shashank Jain
- SANS Incident Handler's Handbook (free download from SANS Reading Room)
- MITRE ATT&CK Framework: `https://attack.mitre.org/`

Tools Used in This Practical

Tool	Purpose	Cost
Python 3.8+	Programming language runtime	Free
Click	CLI framework for command-line interface	Free
Rich	Terminal formatting and styled output	Free
Jinja2	HTML report template engine	Free
PyYAML	Configuration and data parsing	Free
pip	Python package manager	Free

—END OF LAB MANUAL—

Document Version: 1.0

IT Management & Audits – Practical Lab Series