

Information Security and Assurance

laboratory activities

Name | Course Title | Date

**Lab 1: Ransomware Attack Simulation & Incident Response**

**Objective**: Simulate a ransomware attack, analyze its impact, and recover.

**Tools**:

* Virtual Machine (Windows 10)
* Harmless ransomware demo: Hidden Tear (educational use only)
* Wireshark (for network analysis)

**Steps**:

1. Set Up the Lab:

* Install a Windows 10 VM (VirtualBox/VMware).
* Disable Windows Defender temporarily (for testing).

1. Deploy Ransomware (Simulated):

* Download & compile Hidden Tear (C#).
* Run the executable on the VM.
* Observe file encryption and ransom note.

1. Incident Response:

* Detection: Check Task Manager for suspicious processes.
* Containment: Disconnect the VM from the network.
* Analysis:
* Use Wireshark to capture ransomware traffic.
* Check Windows Event Logs (eventvwr.msc) for unusual activity.

1. Recovery & Prevention:

* Restore files from a backup (if available).
* Recommend:
* Regular backups (3-2-1 rule).
* Employee training on phishing emails.

**Deliverable**:

* Incident report with:
* Attack timeline.
* Forensic evidence (logs, network traffic).
* Mitigation strategies.

**Lab 2: Phishing Email Investigation**

**Objective**: Analyze a phishing email and identify threats.

**Tools**:

* GoPhish (for mock phishing campaigns)
* VirusTotal (URL scan)
* Hybrid Analysis (sandboxing)

**Steps**:

1. Set Up GoPhish:

* Install GoPhish on Kali Linux (sudo apt install golang-go).
* Launch the dashboard (./GoPhish).

1. Send a Mock Phishing Email:

* Create a fake "Password Reset" email.
* Embed a harmless malicious link (e.g., http://fake-login-page.com).

1. Analyze the Email:

* Header Analysis: Use Email Header Analyzer (Google).
* Link Analysis: Check on VirusTotal.
* Attachment Analysis: Upload to Hybrid Analysis.

1. Reporting:

* Identify red flags (e.g., mismatched sender domain).
* Recommend email filtering rules (SPF, DKIM, DMARC).

**Deliverable**:

* Forensic report on the phishing attempt.
* Security awareness recommendations.

**Lab 3: Insider Threat (Data Leakage Detection)**

**Objective**: Detect an employee stealing files.

**Tools**:

* Splunk (SIEM)
* FTK Imager (forensics)
* USB Historian (USB tracking)

**Steps**:

1. Simulate Data Theft:

* Have a "rogue" student copy files to a USB.

1. Monitor Logs:

* Use Splunk to track file access (index=security EventID=4663).
* Check USB insertion logs (Get-WinEvent -LogName Security).

1. Forensic Analysis:

* Image the USB with FTK Imager.
* Recover deleted files with Autopsy.

1. Recommendations:

* Enable DLP (Data Loss Prevention).
* Restrict USB usage via Group Policy.

**Deliverable**:

* Insider threat case study.
* Policy recommendations (least privilege).

**Lab 4: Wi-Fi Hacking & Defense**

**Objective**: Crack WPA2 and recommend security improvements.

**Tools**:

* Kali Linux (Aircrack-ng, Wifite)
* Raspberry Pi (optional for rogue AP)

**Steps**:

1. Capture Handshake:

* sudo airmon-ng start wlan0
* sudo airodump-ng -c 6 --bssid [AP\_MAC] -w capture wlan0mon

1. Crack Password:

* sudo aircrack-ng -w rockyou.txt capture.cap

1. Defend:

* Recommend WPA3 or RADIUS authentication.
* Set up a honeypot AP (hostapd).

**Deliverable**:

* Penetration test report.
* Secure Wi-Fi configuration guide.

**Lab 5: Cloud Security Misconfiguration (AWS S3 Bucket)**

**Objective**: Find and fix an exposed S3 bucket.

**Tools**:

* AWS Free Tier account
* ScoutSuite (cloud auditor)

**Steps**:

1. Create a Vulnerable S3 Bucket:

* Set Public Access = ON (for testing).

1. Exploit:

* Access files via curl or browser.

1. Remediate:

* Enable S3 logging.
* Apply bucket policies ("Effect": "Deny").

**Deliverable**:

* Cloud security audit report.

**Lab 6: Digital Forensics (Deleted File Recovery)**

**Objective**: Recover evidence from a disk image.

**Tools**:

* Autopsy
* FTK Imager

**Steps**:

1. Acquire Disk Image:

* dd if=/dev/sdb of=evidence.img

1. Analyze with Autopsy:

* Recover deleted files (Photos, Documents).

1. Timeline Analysis:

* Check $MFT (Master File Table).

**Deliverable**:

* Forensic report with recovered evidence.

**Lab 7: IoT Device Exploitation (IP Camera Hack)**

**Objective**: Hack a vulnerable IoT device.

**Tools**:

* Shodan (shodan search webcam)
* Metasploit (exploit/multi/http/dlink\_upnp\_exec)

**Steps**:

1. Find Device:

* Use Shodan to locate an IP camera.

1. Exploit Default Creds:

* admin:admin login.

1. Recommendations:

* Change default passwords.
* Segment IoT network.

**Deliverable**:

* IoT security assessment.

**Lab 8: Social Engineering (Physical Pen Test)**

**Objective**: Test physical security via tailgating.

**Steps**:

1. Simulate Attack:
   * Try to enter a restricted area without a badge.
2. Defense Training:
   * Teach employees to challenge strangers.

**Deliverable**:

* Physical security audit report.

**Grading Rubric:**

* Technical Execution (40%)
* Reporting (30%)
* Defensive Recommendations (30%)