AJEENKYA
D Y PATIL UNIVERSITY
THE INNOVATION UNIVERSITY

School of Engineering

Seamedu School of Pro-Expressionism	
Task/Project Brief	
Batch Name: Batch 2022	**Department:** BTECH CTIS 6
Task Name: CA - 2	**Subject:** Information Security Applications (Advanced Level)
Date: 4/4/25	**Submission Date:** 14/4/25
Marks: 20	

AJEENKYA D Y PATIL UNIVERSITY
THE INNOVATION UNIVERSITY
School of Engineering

Learning Outcomes:

The following table outlines the specific learning outcomes, the related actions that will be undertaken, and the knowledge that will be leveraged throughout this assessment.

LO	Learning Outcome	In this assessment, you will have the opportunity to present evidence that shows you are able to:
LO1	Understand vulnerability assessment concepts and system hacking techniques.	Demonstrate knowledge of vulnerability classifications, assessment types, and ethical hacking techniques.
LO2	Conduct vulnerability assessment using various tools.	Perform scanning and enumeration using tools like Nessus, OpenVAS, or Nmap.
LO3	Analyze and demonstrate system hacking techniques.	Perform privilege escalation, session hijacking, and DoS attack analysis.
LO4	Identify evasion techniques for IDS, firewalls, and honeypots.	Explore countermeasures against evasion strategies used by hackers.
LO5	Develop security mitigation strategies.	Recommend defense mechanisms against real-world hacking scenarios.

Task Brief

This assignment consists of hands-on activities and research-based exercises that will test your understanding of vulnerability analysis and system hacking techniques.

AJEENKYA D Y PATIL UNIVERSITY
THE INNOVATION UNIVERSITY
School of Engineering

Part A: Hands-On Activities

Task 1: Vulnerability Assessment Simulation

1. Select a vulnerability assessment tool (**Nmap, Nessus, OpenVAS**).
2. Perform a basic scan on a test system (e.g., **Metasploitable, DVWA**).
3. Identify and classify vulnerabilities based on CVSS (Common Vulnerability Scoring System).
4. Submit a brief report including:
    - Identified vulnerabilities
    - Potential impact
    - Suggested mitigation strategies

Task 2: System Hacking & Privilege Escalation

1. Explain the **four stages of system hacking** (**Gaining Access, Privilege Escalation, Maintaining Access, Clearing Logs**).
2. Research a **real-world case study** where a hacker used privilege escalation to gain control.
3. (Optional Practical) Use a **Metasploit Framework** exploit to demonstrate privilege escalation.

Task 3: IDS/Firewall Evasion Research

1. Explore hacker techniques to evade **Intrusion Detection Systems (IDS), Firewalls, and Honeypots**.
2. Demonstrate one method (theoretical or lab-based) such as **IP fragmentation or encrypted payloads**.
3. Suggest security countermeasures.

AJEENKYA D Y PATIL UNIVERSITY
THE INNOVATION UNIVERSITY
School of Engineering

Part B: Attack Simulation

Task 4: Sniffing Techniques & Network Attacks

- Perform a **MAC attack, ARP poisoning, or DNS spoofing** using tools like **Ettercap, Wireshark**.
- Document the attack and propose mitigation strategies.

Task 5: Social Engineering Case Study

- Choose a real-world **identity theft or social media impersonation case**.
- Analyze how the attack was executed and how victims could have prevented it.
- Propose awareness training recommendations.

Task 6: Session Hijacking & Web Application Security

- Demonstrate **session hijacking** using a controlled test environment (e.g., **Burp Suite, Wireshark**).
- Explain **countermeasures** such as HTTPS enforcement, session expiration policies.

Submission Guidelines/Deliverables

Report:

- Submit a **detailed report (PDF format)** covering all research and practical tasks.

- Include **screenshots** of tools used and analysis of results.
- Provide a summary of **findings and mitigation techniques**.

Submission Format:

- Submit only the pdf file named **YourName_CA2.pdf**.
- **Deadline:** 14/4/25

Grading Criteria:

Criteria	Distinction (100%)	Merit (75%)	Pass (50%)	Needs Improvement (25%)	Poor (0%)
Hands-On Activities (5 Marks)	Excellent participation with 100% activities done	Good participation with 75% activities done	Basic participation with 50% activities done	Minimal effort with 30% activities done	Missing or poorly done
Practical Execution (5 Marks)	Strong application of tools with 100% activities done	Good execution with 70% activities done	Basic attempt with 50% activities done	Minimal effort with 30% activities done	Missing or poorly done
Security Countermeasures (7 Marks)	Well-structured and effective strategies	Good strategies with minor gaps	Basic security recommendations	Limited depth and understanding	Missing or poorly done
Uniqueness (3 Marks)	Excellent report	Good report with minor gaps	Basic report with limited depth	Minimal report with weak analysis	Missing or poorly done