UDACITY

Data Security Analysis in Online Payment Processing

Simpson Innocent Nana

6th June, 2024

Section One:
Data Governance

Strategic Data Security Policies

IT Staff should perform a data classification annually, or when there are notable business or technology changes.
Performing a data classification annually, or when significant business or technology changes occur, ensures that JFin Payments can consistently identify and protect sensitive information. This practice helps in maintaining the confidentiality, integrity, and availability of data by categorizing it according to sensitivity and applying appropriate security controls. Regular updates accommodate new types of data and evolving threats, enhancing compliance with regulations such as GDPR and PCI DSS, and supporting effective risk management by prioritizing resources towards the most critical data assets, thus improving operational efficiency.
IT Staff should perform an application and critical system classification annually, or when there are notable business or technology changes.
Conducting an annual classification of applications and critical systems ensures that JFin Payments remains vigilant about which systems are essential to business operations and data security. By regularly assessing and updating the classification, the IT staff can prioritize security measures for the most critical systems, thereby reducing the risk of breaches and downtime. This approach enhances compliance with industry standards, supports robust risk management strategies, and ensures that security efforts are aligned with the organization's evolving technological landscape and business needs, thereby maintaining operational resilience and efficiency.
IT Staff should perform a regulatory assessment annually, or when there are notable business or technology changes.
Performing a regulatory assessment annually, or during notable business or technology changes, keeps JFin Payments in compliance with current laws and regulations such as GDPR, CCPA, and PCI DSS. This proactive approach helps identify and address regulatory gaps, thereby avoiding legal penalties and fostering customer trust. Regular assessments ensure that the company's data security policies are up-to-date with the latest regulatory requirements, contributing to robust risk management. Additionally, it supports operational efficiency by preventing costly compliance failures and ensuring that business processes adhere to the highest standards of data protection.

Data Classification

Confidential: Data whose loss would have a catastrophic impact on the business.
Internal: Data whose loss would have a significant but not catastrophic impact on the business.
Public: Data whose loss would have minimal impact on the business if exposed.

Categorize each dataset into one of the three data types

Dataset	Data Type
Employee profile data	Confidential
Customer profile data	Confidential
Company email	Internal
Repository of previously published blogs	Public
Internal employee newsletters	Internal
Technology engineering diagrams	Internal
Intellectual property	Confidential

Data Regulations

Confidential	General Data Protection Regulation (GDPR): GDPR applies to the processing of personal data of individuals within the European Union. Confidential data like social security numbers or credit card numbers are considered personal data under GDPR. The regulation mandates strict handling, storage, and processing requirements to protect such sensitive information from breaches. Health Insurance Portability and Accountability Act (HIPAA): For organizations dealing with healthcare data, HIPAA sets standards for protecting sensitive patient information. Data such as medical records or health insurance details are classified as confidential and are subject to HIPAA's stringent privacy and security rules to prevent unauthorized access and ensure data integrity. Payment Card Industry Data Security Standard (PCI DSS): PCI DSS applies to organizations that handle credit card information. This regulation enforces security measures to protect cardholder data and prevent fraud. Confidential data like credit card numbers must be secured according to PCI DSS requirements to avoid severe financial and reputational damage.

Data Regulations

Continuation:

Internal	Sarbanes-Oxley Act (SOX): SOX applies to publicly traded companies and mandates rigorous internal controls and procedures for financial reporting. Internal data such as financial statements, internal audit reports, and other non-public financial information must be managed securely to ensure accuracy and reliability, thus preventing fraud and maintaining investor trust.
Public	Freedom of Information Act (FOIA): FOIA applies to federal agencies and ensures public access to government records. Public data, such as published financial reports or official statements, must be accessible to the public under FOIA. This regulation promotes transparency and accountability in government operations.

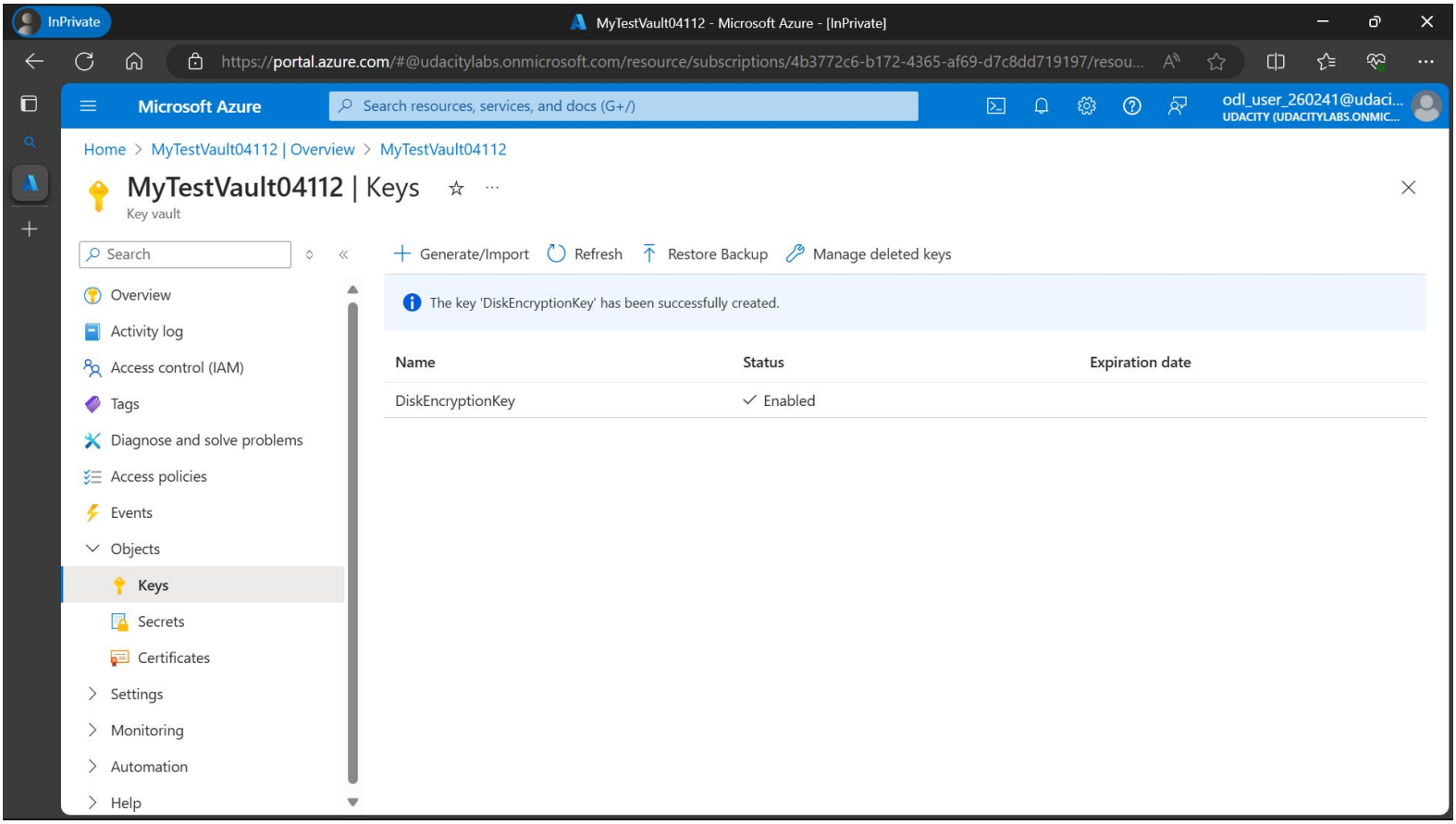
Regulatory Compliance

Encryption Policy: All sensitive data transmitted over internal and external networks must be encrypted using industry-standard encryption algorithms. Encryption keys must be securely managed and periodically rotated to mitigate the risk of unauthorized access and data interception.
Access Control Policy: Access to sensitive data repositories, systems, and applications must be restricted based on the principle of least privilege. Access permissions must be granted only to authorized personnel and reviewed regularly to ensure compliance with regulatory requirements.
Data Retention Policy: A comprehensive data retention schedule must be established to govern the storage and disposal of sensitive data. Data deemed no longer necessary for business or regulatory purposes must be securely erased or destroyed in accordance with applicable data retention regulations.
Incident Response Policy: A documented incident response plan must be in place to address data breaches or security incidents promptly. The plan should outline procedures for detecting, reporting, and responding to security breaches, including notification of affected parties and regulatory authorities as required by law.
Employee Training and Awareness Policy: Regular training sessions and awareness programs must be conducted to educate employees about data security best practices, regulatory compliance requirements, and their roles and responsibilities in safeguarding sensitive information.
Vendor Management Policy: Vendors and third-party service providers handling sensitive data on behalf of JFin Payments must adhere to strict security standards and contractual obligations. Regular audits and assessments should be conducted to ensure compliance with data protection regulations and mitigate third-party risks.

Section Two:
Data Confidentiality

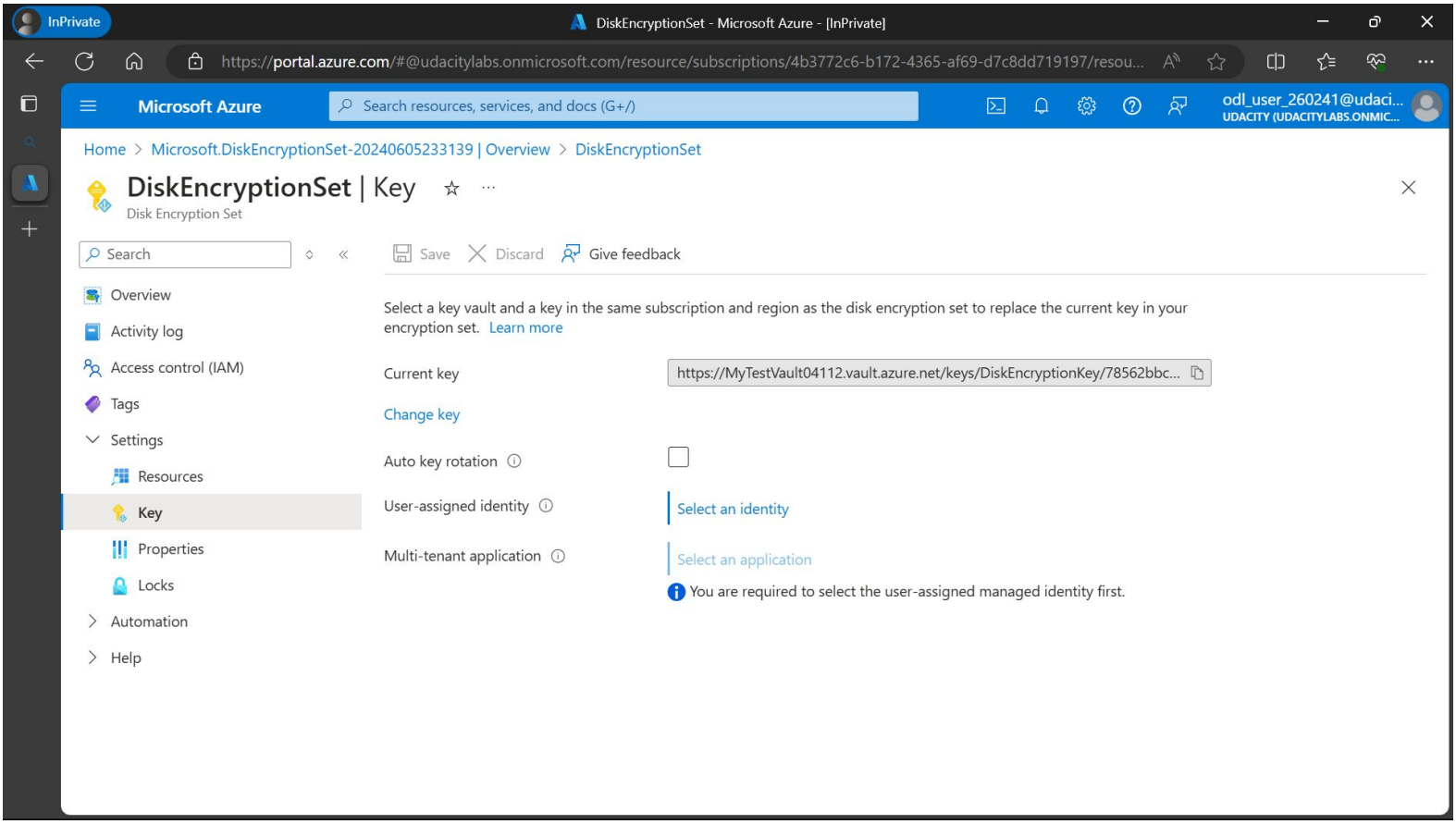
Securing Disks

Place the screenshot from the Keys page of the Key Vault you created, with the generated key.



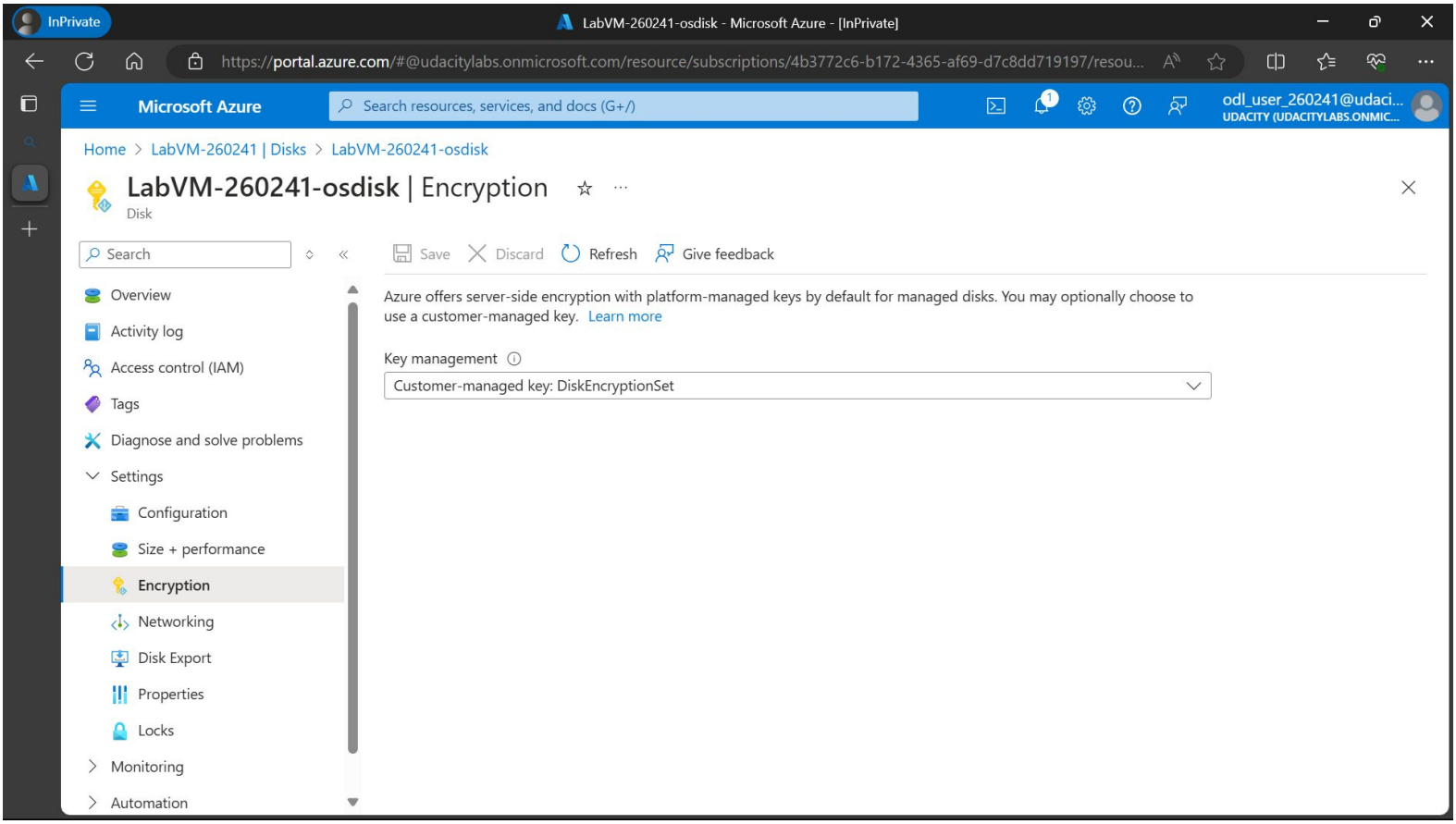
Securing Disks

Place the screenshot from Key page of the Disk Encryption Set you created



Securing Disks

Place the screenshot from the Encryption page of the Disk you created

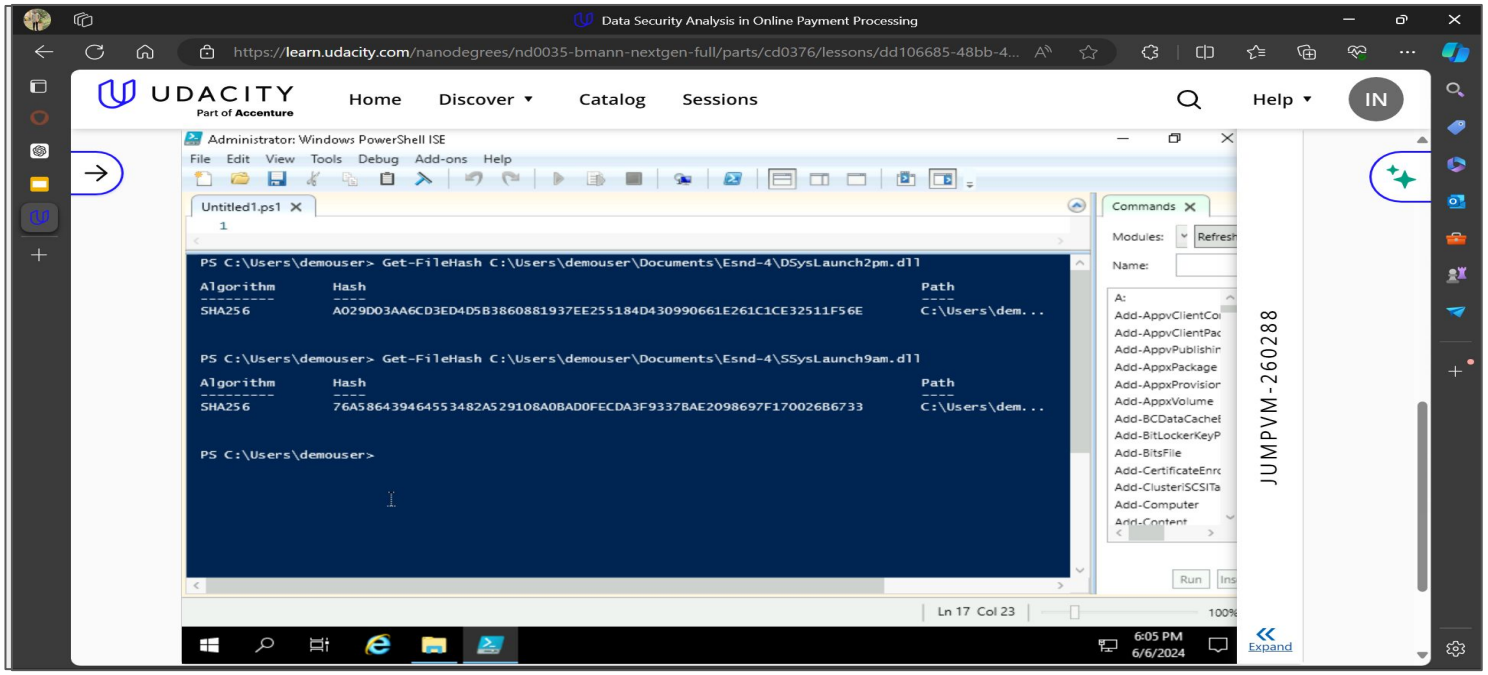


Section Three: Data Integrity

File Integrity Verification

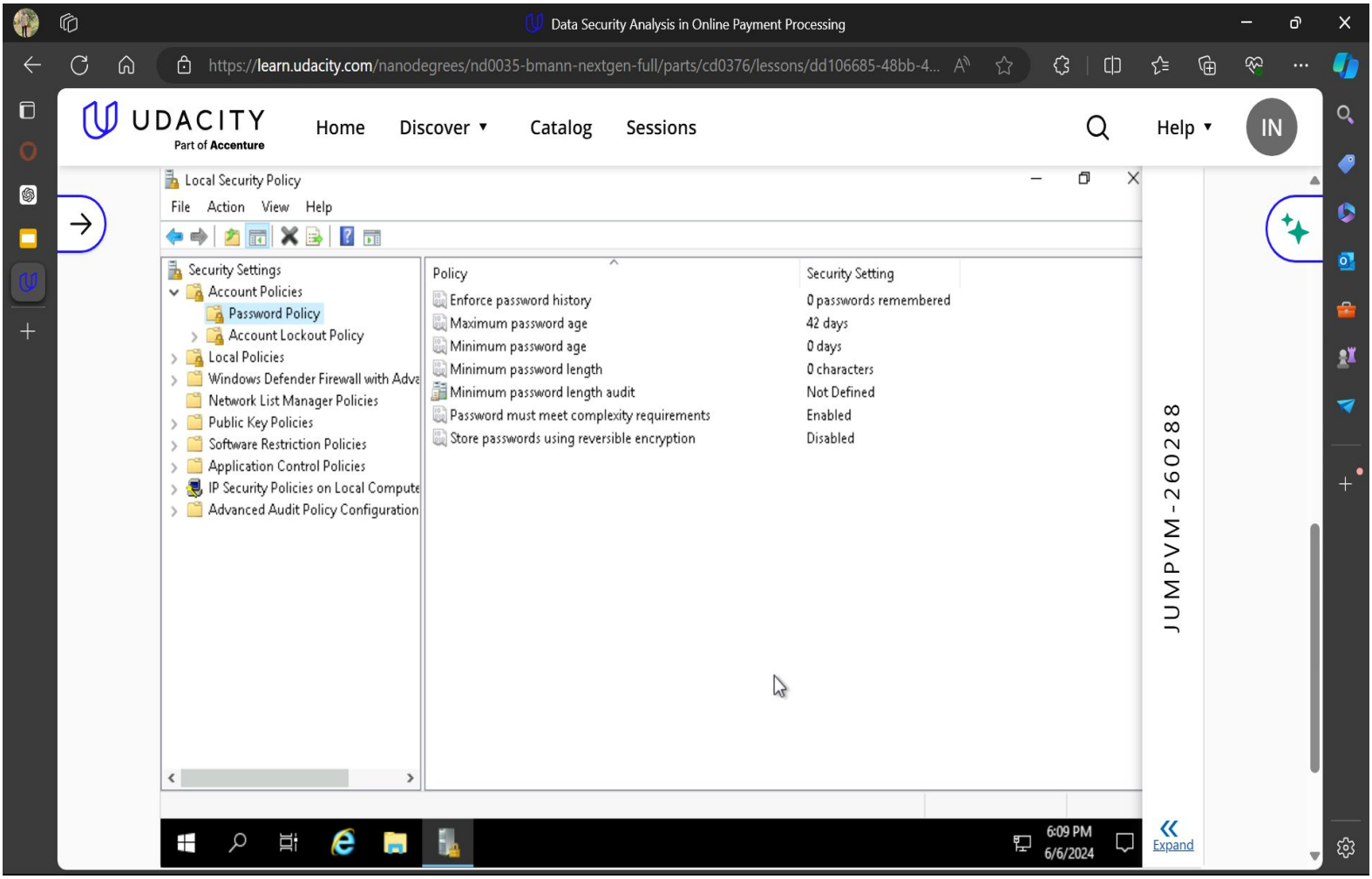
The original DSysLaunch2pm.dll hash: B029D03AA6CD3ED4D5B3860881937EE255184D430990661E261C1CE3251184D4
The original SSysLaunch9am.dll hash: 76A5864394645534 82A529108A0BAD0FECDA3F9337BAE2098697F170026B6733

- The hashes do not match, indicating that the file DSysLaunch2pm.dll has been modified. This discrepancy suggests that the file's integrity has been compromised, meaning it might have been altered or corrupted.
- The hashes match, indicating that the file SSysLaunch9am.dll remains unchanged. This consistency suggests that the file's integrity has been maintained, and it has not been altered or corrupted.



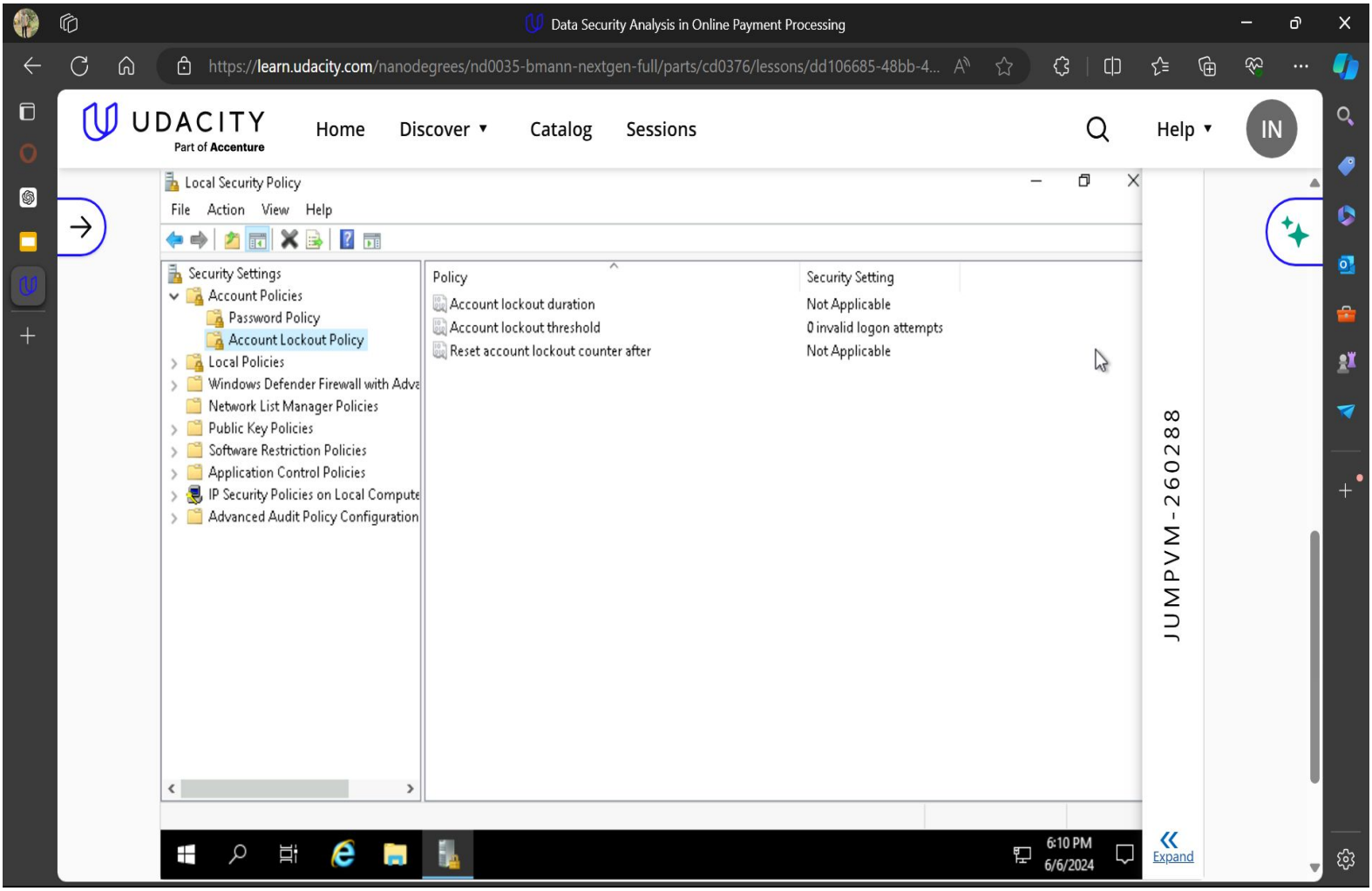
Auditing Security Settings

Place the screenshot of the password policy screen here



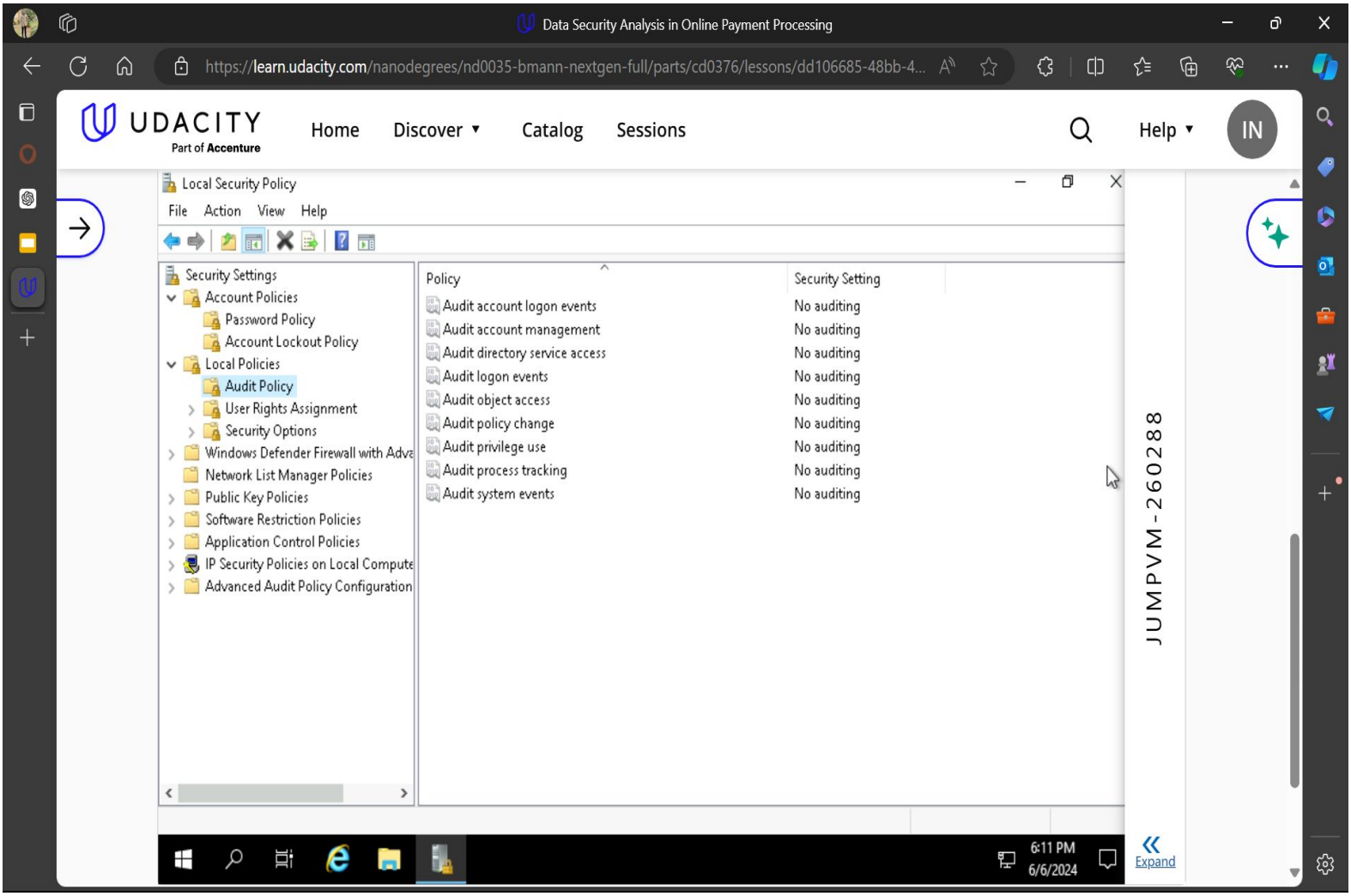
Auditing Security Settings

Place the screenshot of account lockout policy screen here



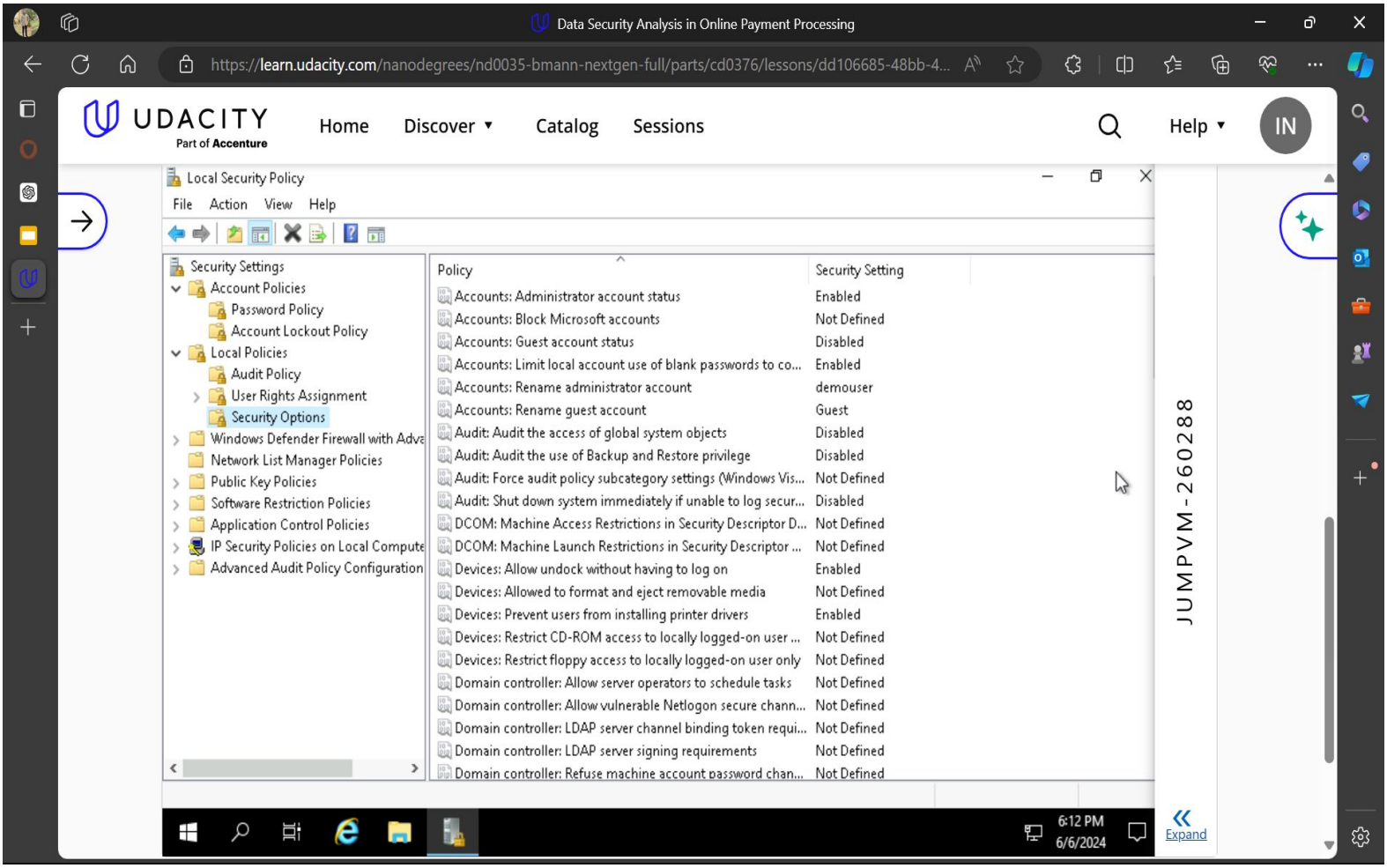
Auditing Security Settings

Place the screenshot of the audit policy screen here



Auditing Security Settings

Place the screenshot of the security options screen here



Enhancing VM Security

1. Implement Strong Password Policies
Implementing a robust password policy ensures that passwords are complex, lengthy, and unique, significantly reducing the likelihood of brute force attacks and unauthorized access. By enforcing password history, users cannot reuse their old passwords, increasing overall security. Shortening the maximum password age ensures passwords are updated regularly, and setting a minimum password age prevents frequent, superficial changes. A minimum length of 12 characters and complexity requirements make passwords harder to crack.
2. Enable Account Lockout Policy
Enabling an account lockout policy helps prevent unauthorized access through repeated login attempts (brute force attacks). By locking accounts after multiple failed attempts, the system deters attackers from guessing passwords. Setting a reasonable lockout duration and counter reset time ensures legitimate users can regain access while providing a deterrent to potential attackers.
3. Enable Comprehensive Audit Policies
Enabling comprehensive auditing helps monitor and record critical actions and events within the system. This allows for the detection of unauthorized access attempts, changes in user accounts, policy modifications, and system events. Logging both successes and failures provides a complete picture of activity, helping in forensic analysis and compliance with regulatory requirements. It also aids in identifying and responding to potential security incidents in a timely manner.

Enhancing VM Security

Continuation:

4. Secure Administrative and Guest Accounts
Renaming the default administrator and guest accounts makes it harder for attackers to target these accounts using common names. Disabling the guest account eliminates a potential entry point that could be exploited. Ensuring the administrator account is enabled and secured with a strong password and monitoring further protects against unauthorized access. These measures add layers of obscurity and control, enhancing overall system security.

Section Four: Data Availability

Developing a Data Backup Strategy

Confidential Data	
Backup Frequency:	Daily
Retention Period:	7 years
Confidential data includes sensitive information such as customer payment details, personally identifiable information (PII), and financial records. Given the criticality of this data, daily backups are essential to ensure minimal data loss in case of a system failure or cyber-attack. Regulatory requirements such as GDPR, PCI-DSS, and other financial regulations often mandate stringent data protection and retention policies. Retaining backups for 7 years aligns with legal obligations and industry best practices, ensuring data availability for audits, compliance checks, and potential disputes.	
Internal Data	
Backup Frequency:	Weekly
Retention Period:	1 year
Internal data includes operational information, employee records, and internal communications, which are important but less critical than confidential data. Weekly backups are sufficient to protect against data loss without overburdening the system. This frequency balances the need for data protection with resource optimization. A retention period of 1 year ensures that internal data is available for operational continuity, internal audits, and regulatory compliance, as some industry standards require maintaining business records for at least a year.	

Developing a Data Backup Strategy

Public Data	
Backup Frequency:	Monthly
Retention Period:	90 Days
Public data includes information available on the company's website, marketing materials, and other non-sensitive data. Since this data is not critical and is often easily reproducible, monthly backups are adequate. This frequency minimizes the risk of data loss while keeping the process efficient and cost-effective. A retention period of 90 days is sufficient for public data, providing a reasonable timeframe to recover from accidental deletions or updates without occupying excessive storage space.	

Creating a Backup

Place the screenshot of the LabVM Backup screen here