DATA SECURITY ANALYSIS

Deekshith A

Project Scenario

Overview

You have recently joined JFin Payments, a rapidly growing online payment processing firm based in Los Angeles, California, as a Data Security Analyst. With over 100,000 **customers across the United States and Europe**, JFin Payments handles a diverse range of sensitive data, including employee and customer profiles, financial information, company communications, and intellectual property.

As a key member of the data security team, your primary responsibility is to ensure the confidentiality, integrity, and availability of the company's data assets. To achieve this, you will collaborate with the data warehouse and application and infrastructure security teams to develop and implement robust data security policies, procedures, and controls.

Throughout the project, you will leverage your expertise in data security, regulatory compliance, and risk management to fortify JFin Payments' data security posture. Your insights and recommendations will play a crucial role in safeguarding sensitive information, maintaining customer trust, and supporting the company's continued growth in the competitive online payment processing industry.

Section 1:

Data Governance

Strategic Data Security Policies

IT Staff should perform a data classification annually, or when there are notable business or technology changes.

Benefits:

- **Enhanced Data Protection:** Identifies and categorizes data based on sensitivity and value, ensuring that high-risk or sensitive data (e.g., customer financial information) receives stronger security controls.
- **Regulatory Compliance:** Supports adherence to privacy laws and industry standards such as PCI DSS, GDPR, and RBI guidelines by ensuring data is appropriately managed.
- **Risk Reduction:** Helps in recognizing obsolete or unnecessary data, reducing the attack surface and minimizing storage of sensitive data that's no longer needed.
- **Operational Efficiency:** Streamlines data handling processes, helping staff prioritize protection efforts based on classification.

Strategic Data Security Policies

IT Staff should perform an application and critical system classification annually, or when there are notable business or technology changes.

Benefits:

- **Focused Security Controls:** Enables prioritization of security resources to mission-critical systems and applications that have the greatest impact on business continuity.
- **Incident Response Readiness:** Helps in developing faster and more accurate incident response strategies by knowing which systems are critical and require immediate recovery.
- **Improved Risk Management:** Ensures that vulnerabilities in high-risk systems are identified and mitigated promptly.
- **Alignment with Business Objectives:** Ensures IT efforts remain aligned with evolving business processes and technological advancements.

Strategic Data Security Policies

IT Staff should perform a regulatory assessment annually, or when there are notable business or technology changes.

Benefits:

- **Maintains Compliance:** Ensures ongoing adherence to legal, financial, and data protection regulations as they evolve, reducing the risk of fines or sanctions.

- **Audit Readiness:** Facilitates internal and external audits by maintaining up-to-date records and demonstrating proactive compliance efforts.

- **Adaptability to Change:** Allows quick adaptation to new regulations introduced due to changes in technology, partnerships, or geographic markets.

- **Strengthens Governance:** Reinforces accountability and structured decision-making in security and compliance efforts.

Data Classification

Confidential: Data that, if disclosed, could cause significant harm to the organization, its employees, or its customers. Access is strictly limited to authorized personnel only. Examples include personal identifiable information (PII), customer financial data, intellectual property, and proprietary systems documentation.
Internal: Data intended for use within the organization that, while not highly sensitive, should not be disclosed to the public. Unauthorized access may cause moderate risk to business operations. Examples include internal communications, employee newsletters, and project planning documents.
Public: Data approved for public distribution. Disclosure poses minimal or no risk to the organization. Examples include marketing materials, public blog posts, and press releases.

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	Confidential
Intellectual property	Confidential

Data Regulations

Confidential	**GDPR (General Data Protection Regulation):** GDPR is the most comprehensive regulation for protecting personally identifiable information (PII), including customer and employee data. It mandates strict controls over the collection, storage, and use of sensitive data, making it highly applicable to confidential datasets
Internal	**ISO/IEC 27001:** ISO 27001 is a global standard for information security management. It provides guidelines for protecting internal business data through access control, risk assessment, and internal audit practices.
Public	**Company Brand and Communications Policy:** While public data isn't regulated by external laws, it must align with internal branding and communication standards to ensure accuracy, consistency, and protection of corporate reputation.

Regulatory Compliance

Data Encryption Policy *All confidential and internal data must be encrypted both at rest and in transit using industry-standard encryption protocols (e.g., AES-256, TLS 1.2 or higher) to prevent unauthorized access and ensure data confidentiality.*
Access Control Policy *Access to confidential and internal data shall be granted strictly on a need-to-know basis and must be protected by multi-factor authentication (MFA). Access rights shall be reviewed and updated quarterly to ensure compliance with role-based access control (RBAC) requirements.*
Data Retention and Disposal Policy *Confidential data must be retained only for as long as necessary to meet business or legal requirements. Upon expiration of the retention period, data must be securely deleted or destroyed using approved data sanitization methods (e.g., DoD 5220.22-M wipe, shredding).*
Breach Notification Policy *In the event of a data breach involving confidential or internal data, the incident must be reported to the Data Protection Officer within 24 hours. If the breach involves personal data, external notification to affected individuals and relevant authorities must be completed within 72 hours in accordance with GDPR requirements.*
Data Classification and Labeling Policy *All data must be classified as Confidential, Internal, or Public at the time of creation or receipt. Each classification must be clearly labeled and handled in accordance with the associated protection requirements.*
Employee Security Awareness Policy *All employees must complete mandatory security awareness training annually, including modules on phishing, secure handling of personal data, and reporting suspicious activities. Compliance with training requirements is tracked and enforced.*

Section 2:

Data Confidentiality

Securing Disks

```
┌──(d33㉿ DESKTOP-B7Q3QFI)-[~]
└─$ ./E-D--Crypto/Encryption\ and\ Decryption/executables/assymetric/ak
Enter the public key file name (.pem): Public.pem
Enter the private key file name (.pem): Private.pem
Enter the RSA key length (e.g., 2048, 3072, 4096): 2048
Public key saved to Public.pem
Private key saved to Private.pem
```

The RSA Key-Pair(2048 bits) is generated using a Custom C++ Script

```
┌──(d33㉿ DESKTOP-B7Q3QFI)-[~]
└─$ cat Public.pem
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxbx4atsNjRlVJcoXdfGz
j6nMp+89nwDLqCTi7CntshyhbKZVLwr9XpFSpqtQRyHSrJEu2t2WoRwNkP/uxWZ0
GvmimQWZnusTqFNhhNr67JdCpQvQezHhH9QHnjs4wFIt2nNHtFUMTqjNu716xxKE
a05jEmZuRbY37RVUMcgdZCOcUU/wVYBtImixrppI484YXiPhnwLSXo3ZDFIrC6EA
UYp9E1m7h1dk/7IBKWOjv7V3TFfqIO/VCpSQJzJLoyjzoB39ZfCwtuMEGLIFqJfT
bygwL1TQJeaH06jFypu3hMUnJrWO7GYSldDXRIgBXzUvNFlteMHCewtxowmZ6rQ4
EwIDAQAB
-----END PUBLIC KEY-----
```

```
┌──(d33㉿ DESKTOP-B7Q3QFI)-[~]
└─$ cat Private.pem
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAxbx4atsNjRlVJcoXdfGzj6nMp+89nwDLqCTi7CntshyhbKZV
Lwr9XpFSpqtQRyHSrJEu2t2WoRwNkP/uxWZ0GvmimQWZnusTqFNhhNr67JdCpQvQ
ezHhH9QHnjs4wFIt2nNHtFUMTqjNu716xxKEa05jEmZuRbY37RVUMcgdZCOcUU/w
VYBtImixrppI484YXiPhnwLSXo3ZDFIrC6EAUYp9E1m7h1dk/7IBKWOjv7V3TFfq
IO/VCpSQJzJLoyjzoB39ZfCwtuMEGLIFqJfTbygwL1TQJeaH06jFypu3hMUnJrWO
7GYSldDXRIgBXzUvNFlteMHCewtx[redacted]/APkCMjPm/W6S
yfB5krFPbNYDu4ns4DQRJnFMBPSHq32UQfnbH4VGq+6/XDqeeb+Rq8YqN+9jGeIS
hy3kVK9yiXt+7Z280AgeIsxIxcsazQVLwkORtafd+dOEItnuTDDegK6UmfW71Cef
ywy+b7xbODbEADQ6SiOPM0sdCeyk36OXDzXSipf4L7lER8eNc2gBzpegwTNP6fJM
GxeYaeNfE+gKZ30qRCbQf3zyyHuPLBBRMzlTcerkiiE2ZRQJ+VlL04AQeqZnjS/G
T7rR+bfUesv2oeDuxn0apTyYbvZJ6EpG3Go7apehvdz9P6LlnVoshNb3WbWM0f3P
/dzkEYECgYEA7gPLSV+II6c0SSucLxUYGe69BWJ+vtSVC8XPIijOfNEfteCtpjG1
kHcOBKb0+bQrj3oyZ5dL5dzrNpy68d6JIC+FceczlT+9deNBWbQETz2UlGCLrgGZ
6nDLrBQ0erM0NcXKts6ewV/YHRd5TAUM5dj12XUuDE9EFsimQ0SyUaECgYEA1K2E
1tq7a6kHy3Mli3PBxccPr3TZrAP18wfHlgArE5AqC1PrKWG9XVk1CF3GqSlWCUcA
oyEH+xuKm3qkKa+MN/fLIfYiv7G8l9PvKYQD52HDa7ms5vW3WUVA55sqqq471msM
mG8UYWkMPKyhc3GcXPnZdUsX4hiGFCWtacxj1TMCgYEAqRDY3Y2WTnz+jtsDXg5F
yGXkrmaAUVz/YhVoRINn6RFCzRaDQoIczjlDI9rUOGraZlgOZbb6mpSKH4jE4fmI
vewDhh0Mbv+PvKVoTieoyACeAadykG9ivTzR77GKdX3FoEyW6bNq4UELad66sl0E
BGBQgd7SjrvfSa/NKgsp/wECgYAbcBNuQKPjXNhDmCRk3FdIc8kDQtj+RziI1R0b
rgPgrz2tXnM9UH3EuEiOPsLtega+hamAYjeMXt4/9s+NDTfS1KYhSIbtIjoJgG8f
dQen50X19OtolJTF8JhSCQO1J2tS21axp8sCUjIg9ciSgzrAB//VEQ4Qvkc1/DJm
LtdGXwKBgGrYwCCtxVcm7qsHXwp6FQg2aM0y69DwqM1XJtsLQs7rV4t0l3mri/9w
fBXq8661PwPiWrQPLm1uiT8YKikYZzs5kMN9JPOEjNkZiFSrfdrG+oJH6F+EZnQp
MSc0huGvRUl6vuCDHwPTecSHUrKJ25FIVDqWxd90auUMdZakOdWO
-----END RSA PRIVATE KEY-----
```

Securing Disks

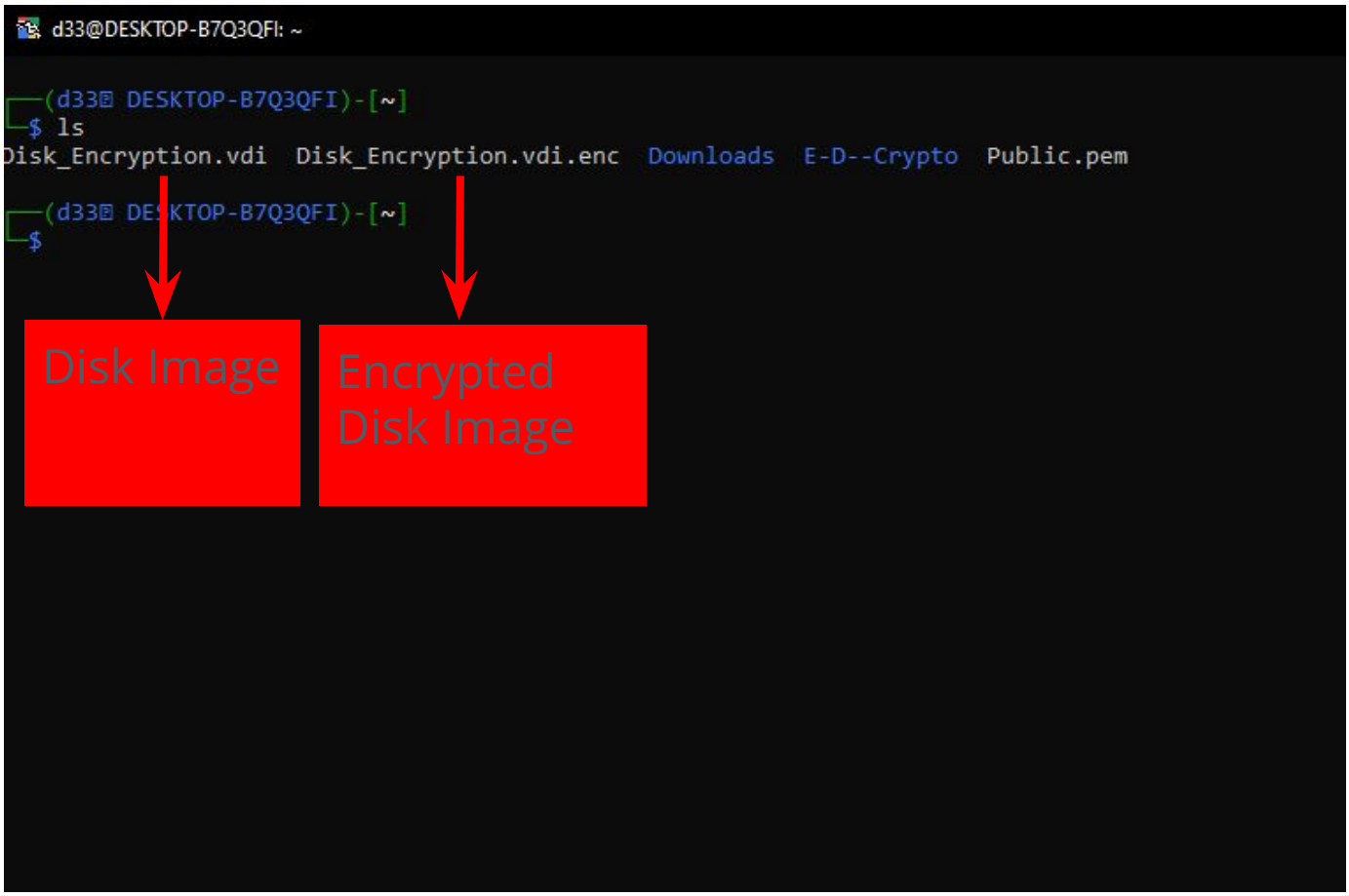
Encrypting The Disk Using a Custom C++ Script via Terminal

```
d33@DESKTOP-B7Q3QFI: ~

┌──(d33㉿DESKTOP-B7Q3QFI)-[~]
└─$ ls
Disk_Encryption.vdi  Downloads  E-D--Crypto  Public.pem

┌──(d33㉿DESKTOP-B7Q3QFI)-[~]
└─$ ./E-D--Crypto/Encryption\ and\ Decryption/executables/assymetric/ae
Enter the input file name: Disk_Encryption.vdi
Enter the output (encrypted) file name: Disk_Encryption.vdi.enc
Enter the public key file name (e.g., public.pem): Public.pem
File successfully encrypted: Disk_Encryption.vdi.enc

┌──(d33㉿DESKTOP-B7Q3QFI)-[~]
└─$
```

```
GNU nano 8.3                                                    encrypt_assymetric.cpp
#include <iostream>
#include <fstream>
#include <vector>
#include <openssl/pem.h>
#include <openssl/rsa.h>
#include <openssl/err.h>

void encryptFile(const std::string &inputFile, const std::string &outputFile, const std::string &publicKeyFile) {
    // Load the public key
    FILE *keyFile = fopen(publicKeyFile.c_str(), "rb");
    if (!keyFile) {
        std::cerr << "Error opening public key file!" << std::endl;
        return;
    }
    RSA *rsa = PEM_read_RSA_PUBKEY(keyFile, nullptr, nullptr, nullptr);
    fclose(keyFile);
    if (!rsa) {
        std::cerr << "Error loading public key: " << ERR_error_string(ERR_get_error(), nullptr) << std::endl;
        return;
    }

    std::ifstream inFile(inputFile, std::ios::binary);
    std::ofstream outFile(outputFile, std::ios::binary);

    if (!inFile.is_open() || !outFile.is_open()) {
        std::cerr << "Error opening input/output file!" << std::endl;
        RSA_free(rsa);
        return;
    }

    const size_t rsaSize = RSA_size(rsa);
    const size_t blockSize = rsaSize - 42; // RSA_PKCS1_OAEP_PADDING
    std::vector<unsigned char> inputBuffer(blockSize);
    std::vector<unsigned char> encryptedBuffer(rsaSize);

    while (inFile.read(reinterpret_cast<char *>(inputBuffer.data()), blockSize) || inFile.gcount() > 0) {
        int inputLength = inFile.gcount();
        int encryptedLength = RSA_public_encrypt(inputLength, inputBuffer.data(), encryptedBuffer.data(), rsa, RSA_PKCS1_OAEP_PADDING);
        if (encryptedLength == -1) {
            std::cerr << "Error encrypting data: " << ERR_error_string(ERR_get_error(), nullptr) << std::endl;
            break;
        }
        outFile.write(reinterpret_cast<char *>(encryptedBuffer.data()), encryptedLength);
    }

    RSA_free(rsa);
    inFile.close();
    outFile.close();
    std::cout << "File successfully encrypted: " << outputFile << std::endl;
}

int main() {
    std::string inputFile, outputFile, publicKeyFile;
    std::cout << "Enter the input file name: ";
    std::cin >> inputFile;
    std::cout << "Enter the output (encrypted) file name: ";
    std::cin >> outputFile;
    std::cout << "Enter the public key file name (e.g., public.pem): ";
    std::cin >> publicKeyFile;

    encryptFile(inputFile, outputFile, publicKeyFile);

    return 0;
}
```

Securing Disks

Successful Creation And Encryption Of the Disk Using The Generated RSA Key(Public key)



Reference:Github
(Contains all required source code and ELF-binaries)

Section 3:
Data Integrity

File Integrity Verification

Version 14.0.0.130

The original public.dll hash:
f7761cd21b7461fd126ecbac1fa7e516138349fb

```
Select d33@DESKTOP-B7Q3QFI: ~
d33@DESKTOP-B7Q3QFI:~$ sha256sum Public.dll
f4876f8f538d0e7c1806e78f0bec57e931d24f7bd29f97841411f16b7d3c51b6  Public.dll
d33@DESKTOP-B7Q3QFI:~$ sha1sum Public.dll
f7761cd21b7461fd126ecbac1fa7e516138349fb  Public.dll
d33@DESKTOP-B7Q3QFI:~$
```

Generated Hash:
SHA256:f48706f8f538d0e7c1806e78f0bec57e931d24f7bd29f97841411f16b7d3c51b6
SHA1:f7761cd21b7461fd126ecbac1fa7e516138349fb

The SHA1 hashes match , the file is legit.

Version 11.4.0.90

The original public.dll hash:
N/A

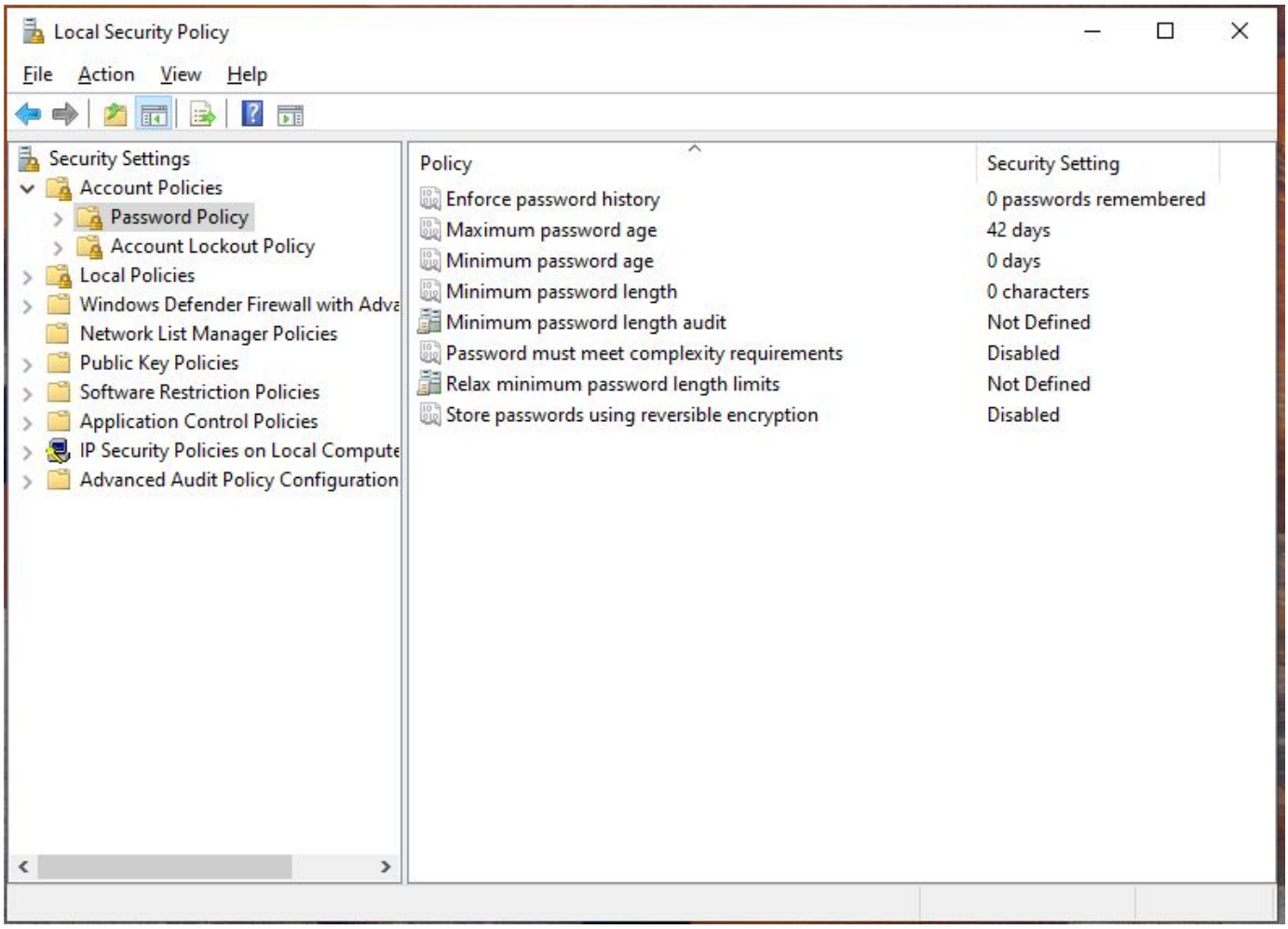
```
d33@DESKTOP-B7Q3QFI: ~
d33@DESKTOP-B7Q3QFI:~$ sha256sum Public.dll
33f71aa1657c045a00f2ae5efc2dddd018caac1edad04b4ad778ad4a85545c9e  Public.dll
d33@DESKTOP-B7Q3QFI:~$
```

Generated Hash:
SHA256:33f71aa1657c645ae00f2ae5efc2dddd018caac1edad04b4ad778ad4a85545c9e

The File Public.dll(version 11.4.0.90) cannot be concluded as compromised or not since the original hash is Unknown.

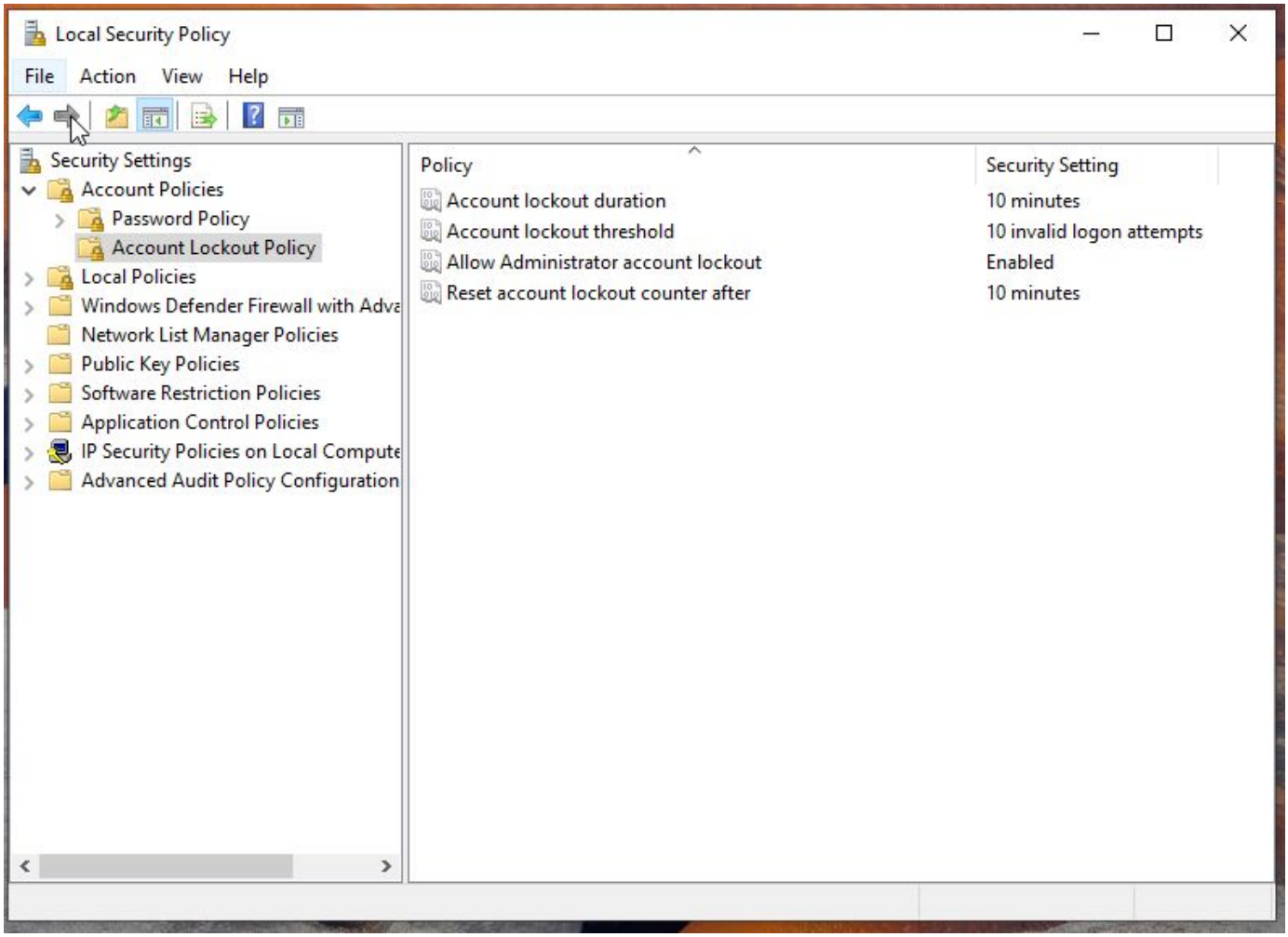
Auditing Security Settings

Password Policies



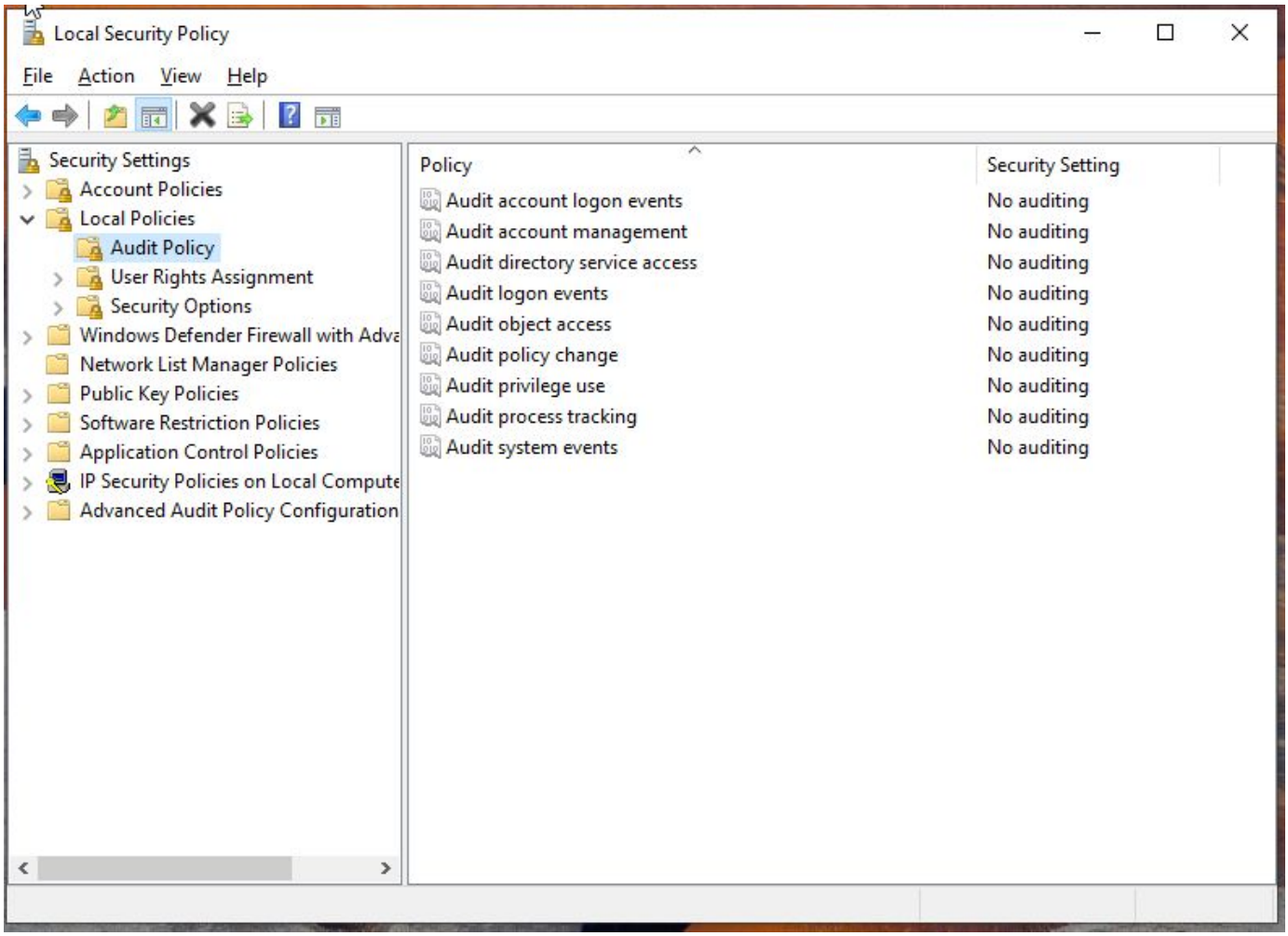
Auditing Security Settings

Account Lockout Policy



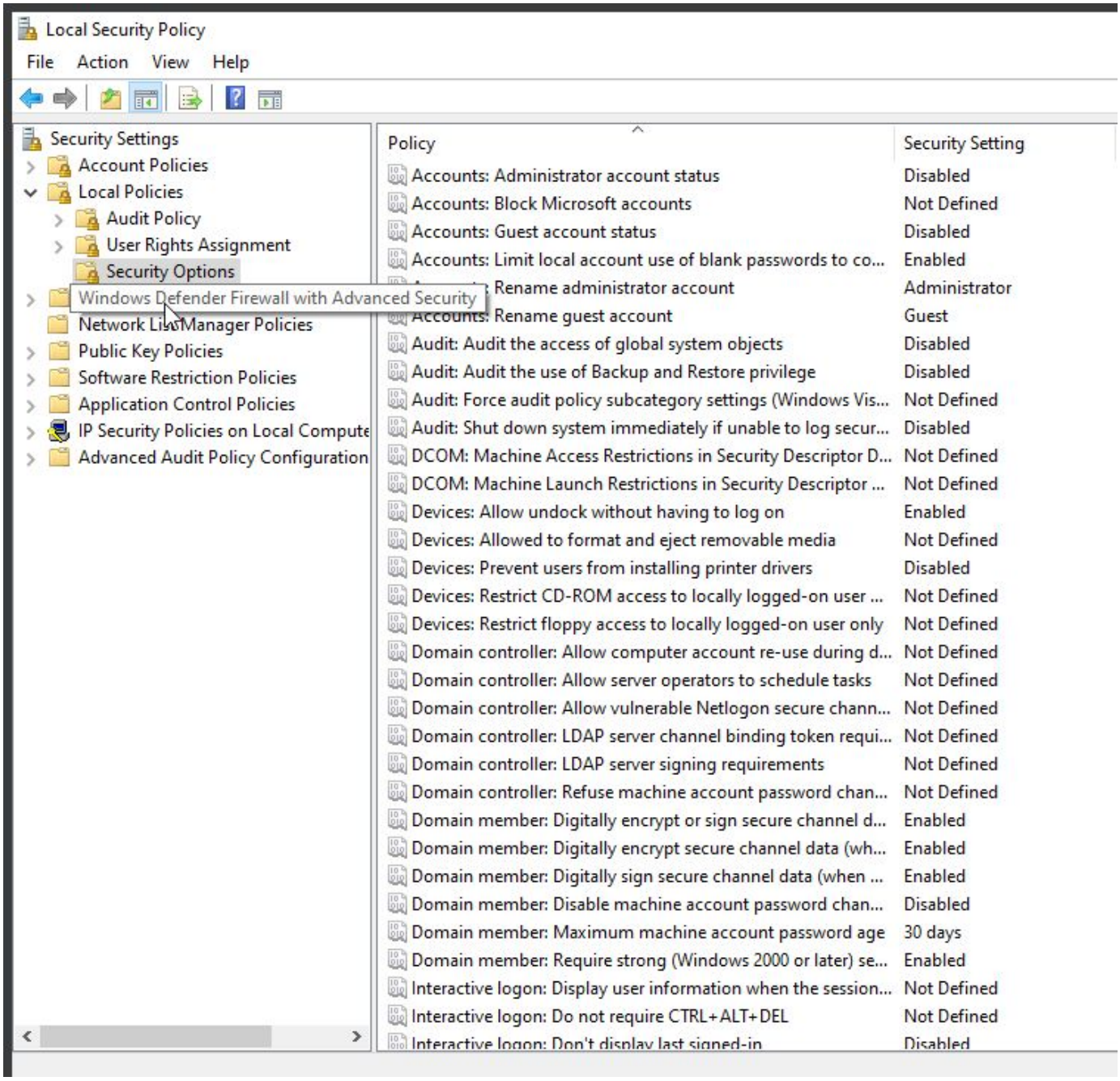
Auditing Security Settings

Audit Policy



Auditing Security Settings

Security Options
There are a Total of 181 policies



Enhancing VM Security

Enforce Stronger Password Policies

Recommendation:

Set the following under **Local Security Policy > Account Policies > Password Policy:**

- Minimum password length: **12 characters**
- Password complexity: **Enabled**
- Maximum password age: **60 days**
- Minimum password age: **1 day**
- Enforce password history: **Remember last 24 passwords**

Justification:

This reduces the risk of brute-force attacks and prevents users from reusing weak or compromised passwords. Enforcing complexity and history requirements helps maintain password hygiene and meets common compliance requirements (e.g., CIS Benchmarks, NIST).

Enhancing VM Security

Configure Account Lockout Threshold

Recommendation:

Under **Account Lockout Policy**, set:

- Account lockout threshold: **5 invalid attempts**
- Account lockout duration: **15 minutes**
- Reset account lockout counter after: **15 minutes**

Justification:

This helps prevent unauthorized access from password-guessing or brute-force login attempts. Temporarily locking the account discourages repeated attacks while balancing user convenience.

Enhancing VM Security

Enable Full Audit Logging

Recommendation:

Enable and configure **Audit Policy** settings to track critical system activities:

- Audit logon events: **Success and Failure**
- Audit object access: **Failure**
- Audit account logon events: **Success and Failure**
- Audit system events: **Success and Failure**

Justification:

Audit logs are essential for incident detection and forensic analysis. Enabling both success and failure events gives visibility into normal activity and potential malicious behavior, aiding compliance with standards like ISO 27001 and NIST SP 800-53.

Enhancing VM Security

Harden Security Options

Recommendation:

Under **Local Policies** > **Se**curity Options, configure the following:

- Accounts: **Administrator account status** → **Disabled**
- Accounts: **Guest account status** → **Disabled**
- User Account Control: **Run all administrators in Admin Approval Mode** → **Enabled**
- Network security: **Do not store LAN Manager hash value on next password change** → **Enabled**

Justification:

Disabling unnecessary default accounts (Administrator, Guest) limits attack surfaces. Enabling UAC for admins reduces the chance of privilege misuse. Disabling LAN Manager hash storage ensures stronger password hashing to prevent offline cracking attacks.

Section 4:
Data Availability

Developing a Data Backup Strategy

Confidential Data	
Backup Frequency:	Real-time (or at least Daily)
Retention Period:	7 Years

Justification:

- **Critical business data** such as customer financial records, personally identifiable information (PII), and payment card data falls under this category.
- Regulations such as **PCI DSS, GDPR,** and **local financial data laws** require **data integrity, availability, and long-term retention.**
- **Real-time or daily backups** reduce the risk of data loss, while **7-year retention** aligns with common financial regulations and audit requirements.
- Real-time backup can be achieved via continuous data protection (CDP) or replication to secure offsite/cloud locations.

Developing a Data Backup Strategy

Internal Data	
Backup Frequency:	Daily
Retention Period:	90 Days

Justification:

- Includes internal reports, process documentation, training materials, and employee communications.
- Although not as sensitive as confidential data, loss can **disrupt operations** or **impede audits.**
- Daily backups ensure up-to-date copies without unnecessary storage overhead.
- A **90-day retention** balances compliance (e.g., internal audit readiness) and **cost efficiency.**

Developing a Data Backup Strategy

Public Data	
Backup Frequency:	Weekly (or As Needed)
Retention Period:	30 days

Justification:

- Includes content meant for public release such as press releases, marketing materials, and website content.
- Loss of this data is less damaging and often retrievable from other sources.
- **Weekly backups** are sufficient, with **30-day retention** providing enough buffer for recovery from accidental deletion or unauthorized changes.

Creating a Backup

Backing up using Powershell Script Locally

Command:

Copy-Item "C:\Users\d33\VirtualBox VMs\Ububtu" "C:\Users\d33\VirtualBox VMs Backup\Ububtu_$(Get-Date -Format yyyyMMdd)" -Recurse