Lab 7 Implementing an IT Security Policy

Osamudiamen Eweka

Cyb-605-Z2 Principles of Cybersecurity

Utica University

Introduction

In every organization, the collective effort of all employees is crucial for maintaining security, yet the leadership has a pivotal role in establishing and upholding a robust security framework. The leadership not only outlines the vision and allocates the necessary resources for implementing the information security strategy, but also influences the organizational culture towards security. Defining clear objectives through an Information technology (IT) security policy is a foundational step in this strategy, which reflects the leadership's expectations and shapes the organization's security ethos.

An IT security policy should not be seen as a singular document but rather as a structured collection of documents catering to various aspects and levels within the organization. At its core, the organizational level policy encapsulates the ethos and tone towards security, branching out into functional policies that guide specific management activities, such as acceptable use, antivirus measures, and mobile device management (Habte, 2021). These policies are supported by standards, procedures, baselines, and guidelines that offer detailed directions and recommendations for practical implementation.

This hands-on lab emphasizes the practical application of different functional security policies using tools like Microsoft's Group Policy Management Console. Participants will gain experience in enforcing password protection, antivirus policies, and the deployment of security baselines, alongside understanding the best practices for securing mobile devices, thereby offering a comprehensive skill set for managing an organization's security posture effectively.

Objective

The objective of this lab report is to systematically explore and implement critical IT security policies within a simulated organizational environment. This entails the practical application of password protection, antivirus strategies, and Windows security baselines to safeguard digital assets. Additionally, the report aims to analyze and develop Acceptable Use Policies and Privacy Policies, focusing on their essential role in regulating access to company resources, protecting sensitive data, and ensuring user privacy. Through hands-on experiments and theoretical analysis, the report seeks to enhance the understanding of effective IT security measures and their impact on organizational security posture.

Lab Setup

The Tools and Software section lists essential software and utilities for completing the lab, emphasizing the importance of hands-on experience with real-world IT security tools. Students are encouraged to use:

- **Group Policy Management Console (GPMC)**: A Microsoft management tool used to manage Group Policy settings.
- **Active Directory Users and Groups**: A tool within Windows Server to manage users and groups, central to managing access and security policies.
- **Windows Defender Antivirus**: Microsoft's integrated antivirus protection for Windows, crucial for defending against malware and cyber threats.
- **Security Compliance Toolkit (SCT)**: A set of tools provided by Microsoft that enables security professionals to assess and enforce compliance with security best practices.

These tools are foundational for understanding and implementing IT security measures in a practical setting, providing students with hands-on experience in managing and securing IT environments.

Section 1

Part 1: Implement a Password Protection Policy

Implementing a password protection policy within an organization is a critical step towards ensuring IT security. This process typically begins with defining the policy's parameters, such as password complexity requirements, expiration timelines, and the procedures for password changes and resets. In a Microsoft Windows environment, these policies can be efficiently enforced using Active Directory and the Group Policy Management Console (GPMC).

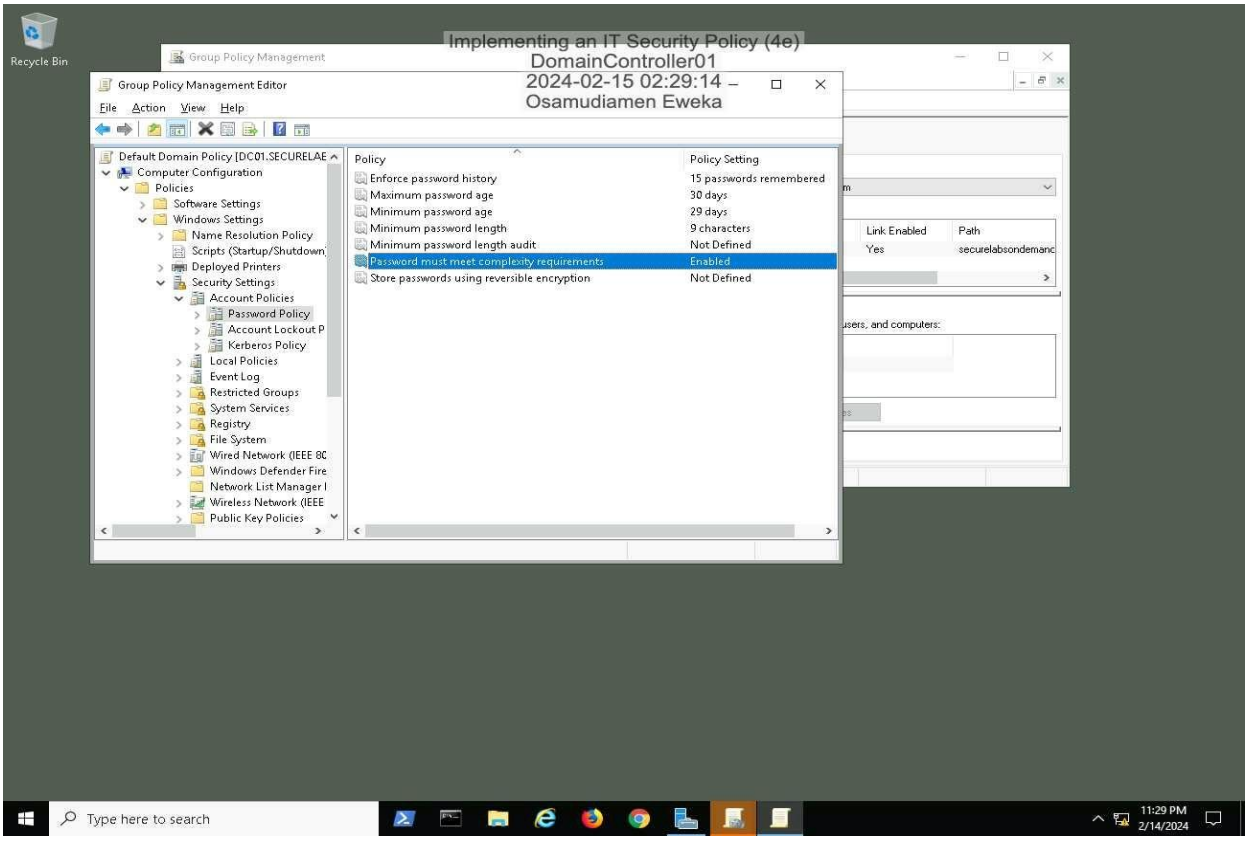
Active Directory serves as a centralized database for user and device settings, while GPMC allows for the management of Group Policy Objects (GPOs) that apply these settings across a domain. To implement a password policy, an administrator would access the GPMC on a Domain Controller, navigate to the appropriate domain, and edit the Default Domain Policy or create a new GPO tailored to the organization's needs.

The key settings adjusted in the password policy include enforcing password history to prevent the reuse of old passwords, setting the maximum password age to mandate regular password changes, defining the minimum password length to ensure passwords are sufficiently complex, and enabling complexity requirements to include a mix of character types in each password.

By leveraging these tools and settings, organizations can align their IT infrastructure with internal security policies, providing a robust defense against unauthorized access and enhancing overall security posture. Figure 1 illustrates this process (Jones & Bartlett, 2024).

Figure 1

Make a screen capture showing the newly configured Domain Password Policy settings.



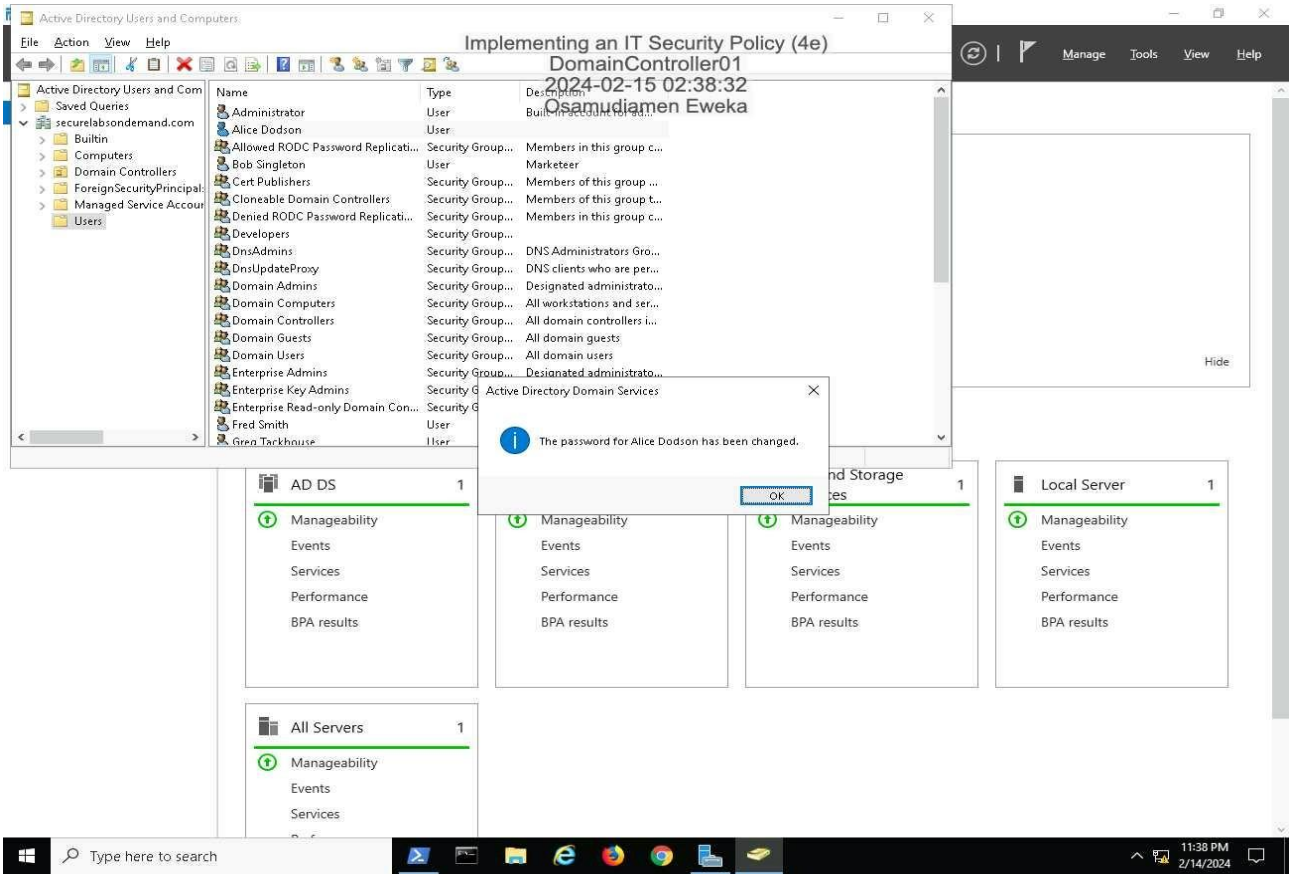
it's pivotal to delve into the intricacies of each step involved in updating and enforcing the new password policy within an Active Directory environment, post-policy adjustment. After amending the password policy, executing gpupdate /force via PowerShell is crucial for the immediate application of Group Policy updates across the domain controller. This command synchronizes the domain controller with the newly established policies, ensuring all changes are propagated effectively.

The subsequent step involves utilizing the Active Directory Users and Computers console, a vital tool for domain administrators managing user identities and access controls. By navigating to this console, administrators can directly apply the updated policy through practical actions, such as resetting a user account password, to demonstrate the policy's enforcement.

This process exemplifies the procedural rigor required in managing IT security policies within an organizational infrastructure. It underscores the utility of Active Directory in centralizing and streamlining access management, aligning with the broader objective of maintaining robust security protocols. Through these detailed steps, one can appreciate the comprehensive approach needed to enforce security policies effectively, ensuring adherence to updated standards and enhancing the overall security posture of the organization As shown in Figure 2 (Jones & Bartlett, 2024).

Figure 2

Make a screen capture showing the successful password change message.



In this detailed explanation, we examine the process of logging into a workstation following the enforcement of updated password policies within the Active Directory

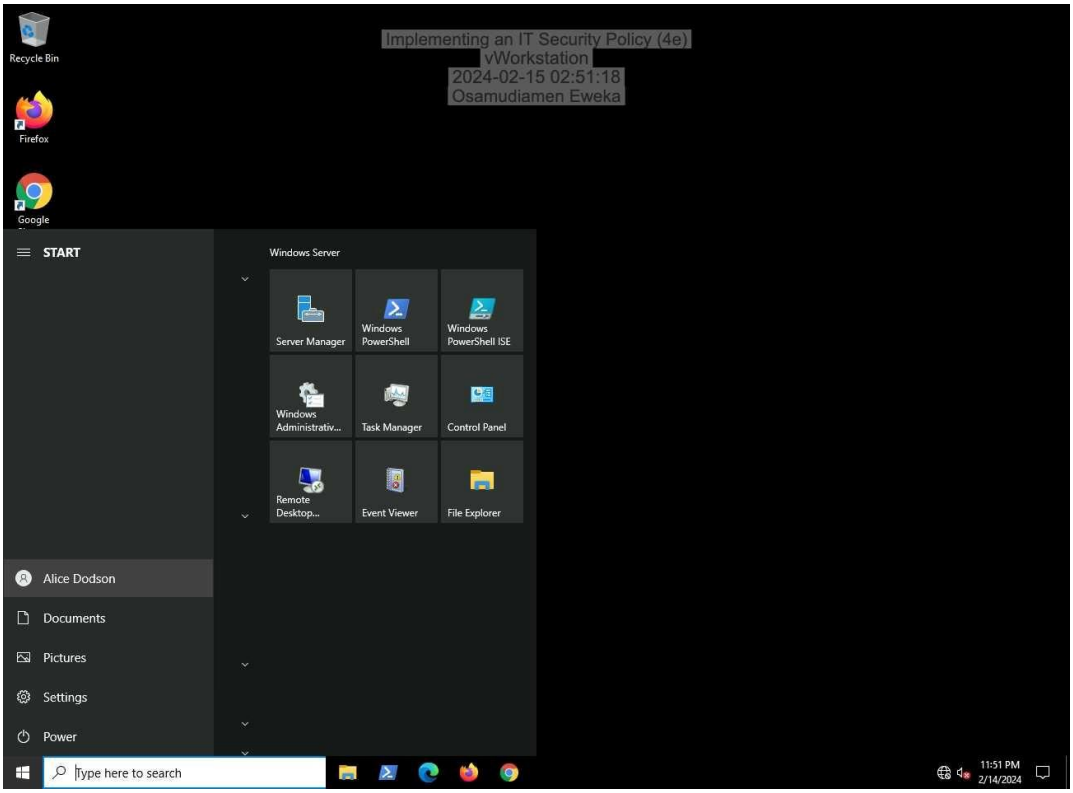
environment of securelabsondemand.com. The policy changes, including the enforcement of complex password requirements, were applied through the Group Policy Management Console and are now being tested by logging into a workstation with a user account that complies with the new password standards.

The nuances of policy application in Active Directory, such as the "Link enabled" and "Enforced" settings, are crucial for ensuring that the desired policy settings are applied across the domain without being overridden by more granular GPOs linked to specific organizational units or groups. This hierarchical approach to policy management allows for a balance between global policy enforcement and the flexibility to address specific requirements within different parts of the organization.

Logging into the vWorkstation using the updated credentials of a sample user account demonstrates the practical application of these policy changes, serving as a validation of the policy enforcement mechanism. This process not only underscores the technical steps involved in managing and applying GPOs but also highlights the importance of user education and policy adherence in maintaining security. Despite the implementation of technical controls, the effectiveness of security measures heavily relies on user behavior and awareness, emphasizing the need for ongoing security education and a culture of security within the organization. Figure 3 shows the successfully logged on user account (Jones & Bartlett, 2024).

Figure 3

Make a screen capture showing the logged-on user account.



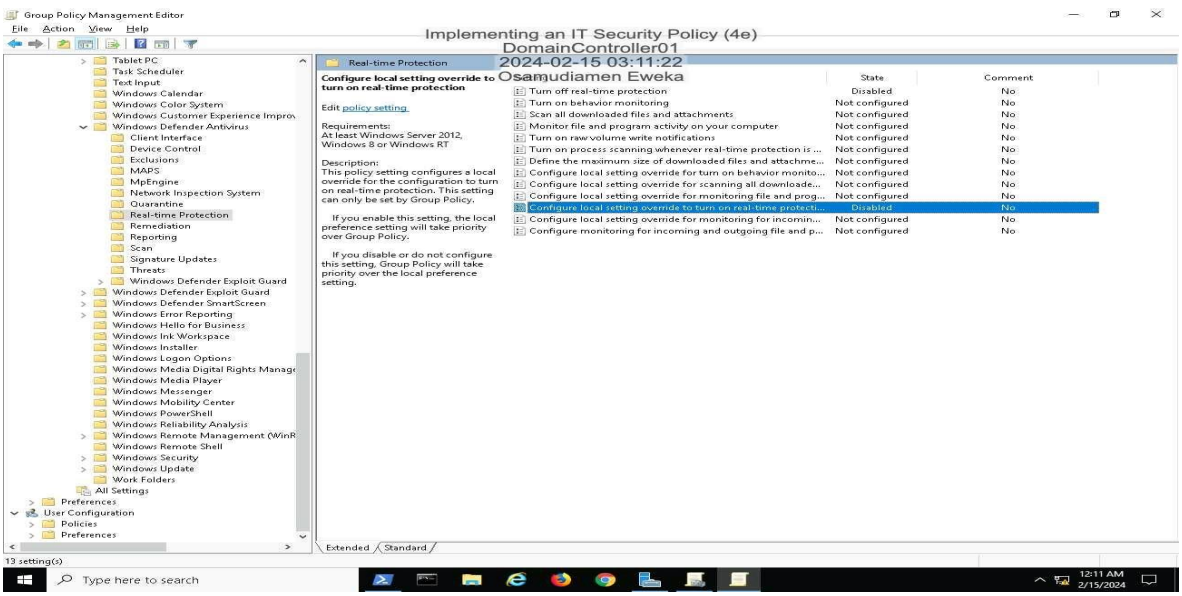
Section 1

Part 2: Implement an Antivirus Policy

In this lab section, the focus shifts to implementing an antivirus policy using Active Directory and Group Policy Management Console (GPMC) to manage Windows Defender Antivirus settings centrally. The procedure involves navigating through the GPMC to access and modify the Real-time protection settings, ensuring that it remains always on for all domain-connected devices, thereby prohibiting local overrides. This centralized management approach underscores the efficiency of using Active Directory to enforce security policies across an organization, demonstrating the practical application of GPOs in maintaining system integrity and combating malware. The lab illustrates the critical role of real-time protection in a comprehensive anti-malware strategy, emphasizing its necessity in preemptively blocking potential threats. Figure 4 shows the new real-time protection policy settings (Jones & Bartlett, 2024).

Figure 4

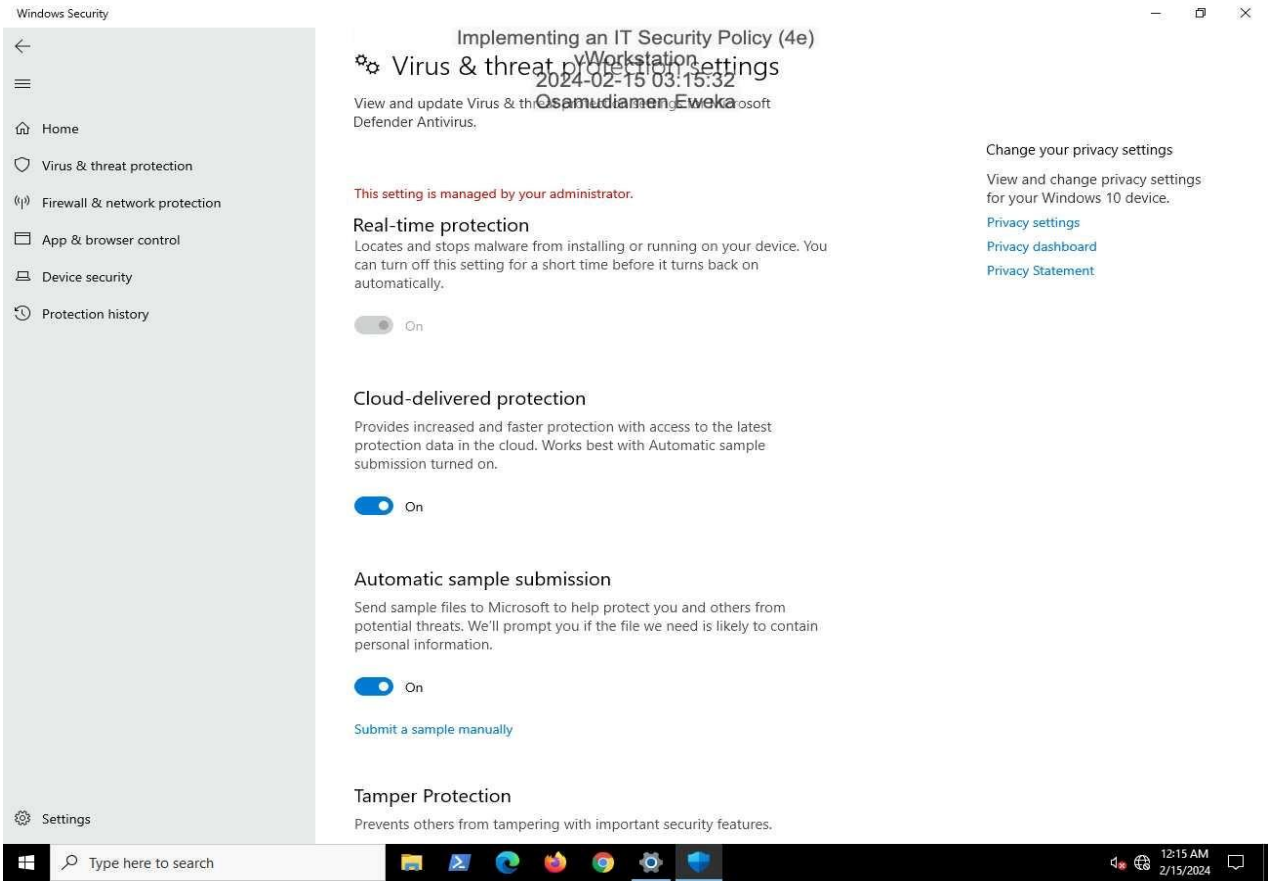
Make a screen capture showing the newly configured Domain Real-time protection Policy settings.



The screenshot in Figure 4 confirms that the Group Policy for antivirus settings has been successfully applied to the workstation (Jones & Bartlett, 2024). The real-time threat protection settings are displayed as grayed out, indicating that they are being managed by the domain controller and are not editable at the user level. This illustrates the centralized control over antivirus policies and highlights the security benefit of such management, as it ensures consistency in protection across all devices in the domain. This step is a crucial component of the broader antivirus strategy, emphasizing the centralized enforcement of security measures over-reliance on end-user compliance.

Figure 5

Make a screen capture showing the grayed-out real-time threat protection settings.



Section 2

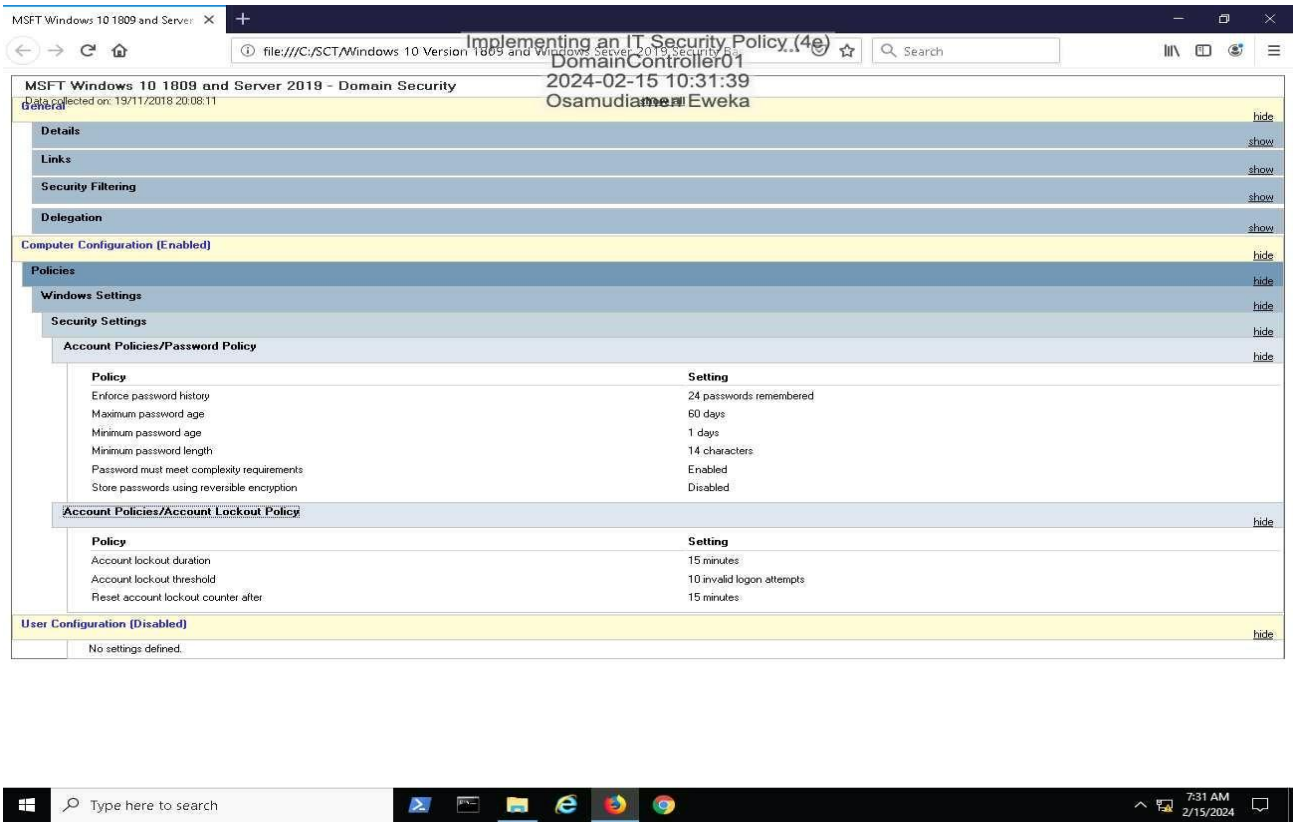
Part 1: Apply a Windows Security Baseline

In this lab segment, you'll explore a more streamlined approach to enforcing a password protection policy and other domain-level policies using Active Directory and the Group Policy Management Console. Microsoft's Security Compliance Toolkit offers security baselines, which are collections of recommended configuration settings for Windows operating systems, derived from insights by Microsoft's security teams and their partners. These baselines, consisting of (GPOs), facilitate the secure configuration of Windows environments. You'll learn to use these baselines alongside tools like the Policy Analyzer to enhance your Group Policy settings, tailoring them to your organization's specific requirements and deploying them via the Microsoft Group Policy Management Console. The exercise involves creating a new GPO on DomainController01, importing a Domain Security baseline for Server 2019, and linking it to your domain.

Participants are guided through the process of examining the Password and Account Lockout Policy settings within the Group Policy Report for Microsoft's recommended domain security policies. These settings are crucial for enhancing security by making it difficult for attackers to guess or compromise passwords through automated methods. The Account Lockout Policy is designed to temporarily lock accounts after a specified number of failed sign-in attempts, a measure that helps prevent automated password attacks. Administrators can configure settings such as the threshold for failed sign-in attempts, the duration of the lockout, and the reset period for the count of failed attempts. Figure 6 captures the recommended Password and Account Lockout policy settings (Jones & Bartlett, 2024).

Figure 6

Make a screen capture showing the Microsoft's recommended Password and Account Lockout policy settings.

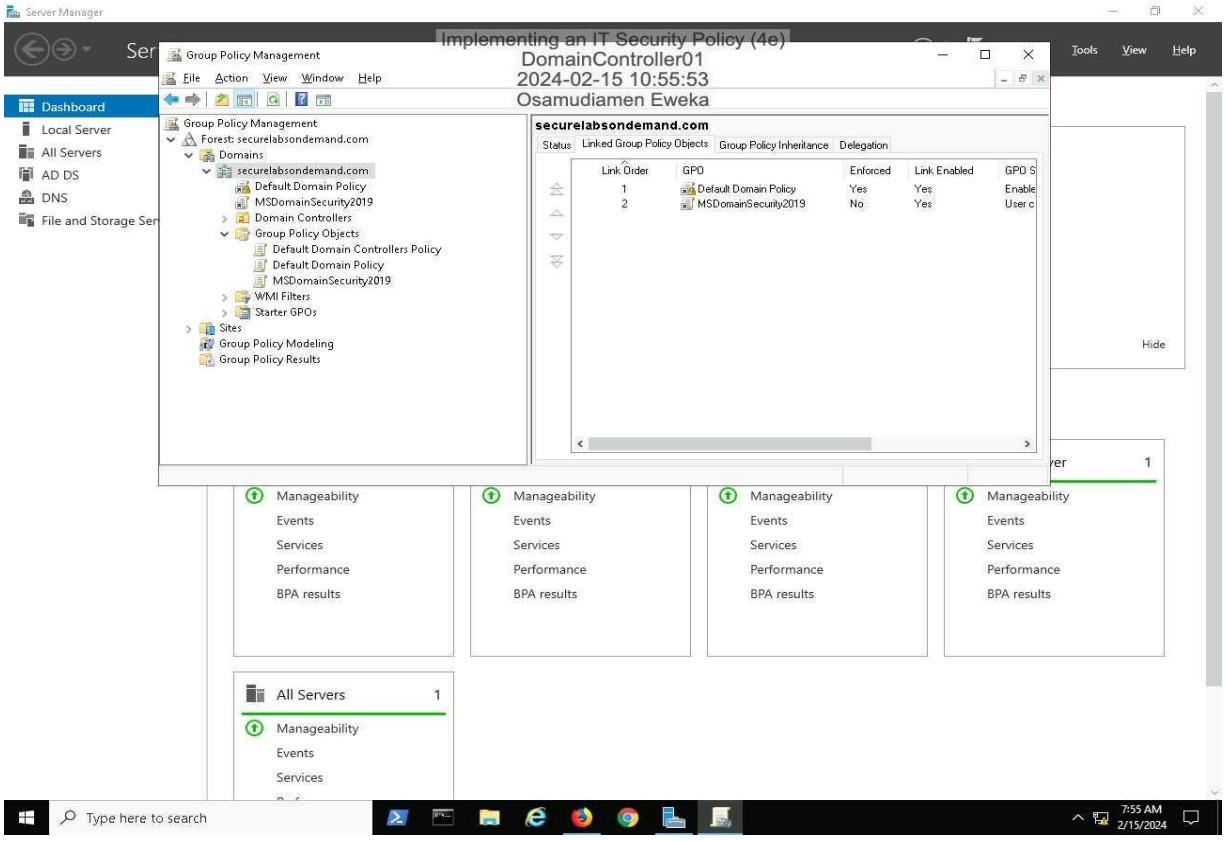


Participants go on to open a Group Policy Management Console, creating a new GPO titled 'MSDomainSecurity2019', and importing settings from a pre-configured backup, specifically the Microsoft Windows security baseline for Server 2019, from the Security Compliance Toolkit. Instead of backing up the new GPO, Participants proceeded directly to import the settings since this GPO is newly created and empty. After selecting the appropriate backup from the SCT directory, you scan the backup file, finalize the import, and then link this new GPO to the 'securelabsondemand.com' domain. This process centralizes security configurations, making the management of domain-level security settings more streamlined and

efficient. The final step involves making a screen capture to document the linked GPO within the Group Policy Management Console, evidencing that the 'MSDomainSecurity2019' GPO is now actively linked to the domain this screen capture can be seen in Figure 7 below (Jones & Bartlett, 2024).

Figure 7

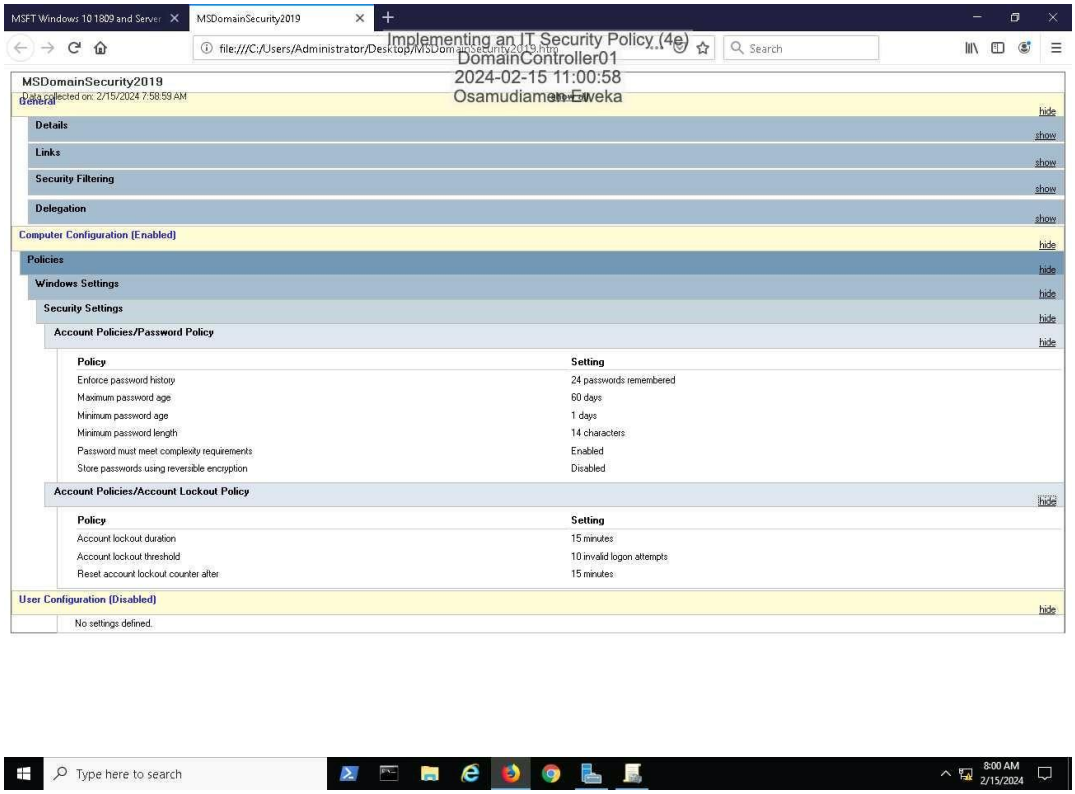
Make a screen capture showing the linked MSDomainSecurity2019 object.



Participants are to Save the GPO Report to the DomainController01 desktop as MSDomainSecurity2019_report, Open the MSDomainSecurity2019_report, and locate the Password and Account Lockout policy settings as illustrated below in Figure 8 (Jones & Bartlett, 2024).

Figure 8

Make a screen capture showing the Password and Account Lockout policy settings.



Section 2

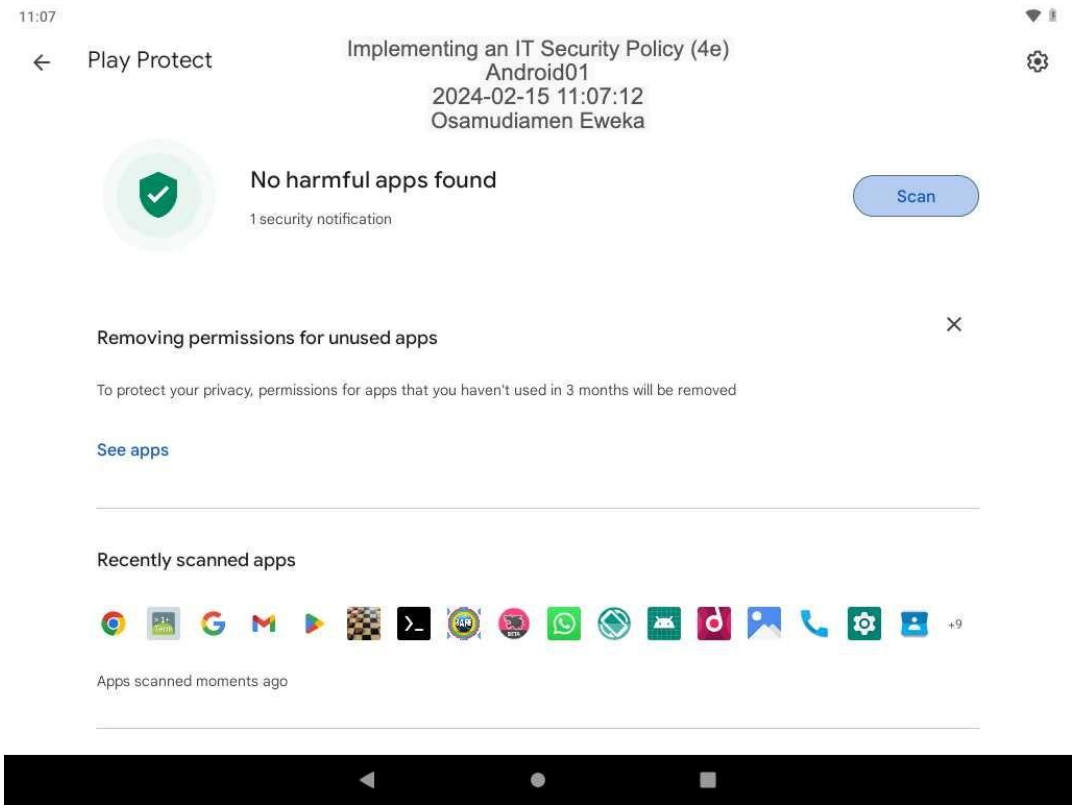
Part 2: Implement a Mobile Device Security Policy

In the context of modern IT infrastructure, where mobile devices are prevalent and often dual-purpose, serving both personal and organizational functions, the implementation of a stringent mobile device security policy is imperative. Such a policy delineates the minimum security standards necessary for these devices to connect to an organization's network securely. For Android devices, the policy mandates the activation of Google Play Protect to perform daily scans for malicious software. Additionally, it requires users to regularly check for and install security updates within a prescribed timeframe, use a password to secure the lock screen, and enable full device encryption to safeguard data in case the device is lost or stolen. Moreover, the 'Find My Device' feature must be activated to assist in locating the device or wiping its data remotely if necessary. Through the lab activity, these protocols are meticulously applied to an Android device, thereby aligning it with the organization's security requirements and mitigating the risks introduced by the widespread utilization of mobile devices in corporate environments.

The screen capture in figure 9 displays the results of a Google Play Protect scan on an Android device. It indicates that the scan was successful and that "no harmful apps were found" (Jones & Bartlett, 2024). This notification shows that Google Play Protect is actively safeguarding the device by scanning for potentially harmful apps, aligning with the mobile device security policy's requirements. It also shows the option to conduct a new scan, further emphasizing the ease of ongoing device security management.

Figure 9

Make a screen capture showing the results of the Google Play Protect scan.



In navigating the Android Version 9 Security & Location settings, a critical initial step involves returning to the primary security settings by selecting the Triangle icon, emphasizing the importance of frequent security updates for device safety.

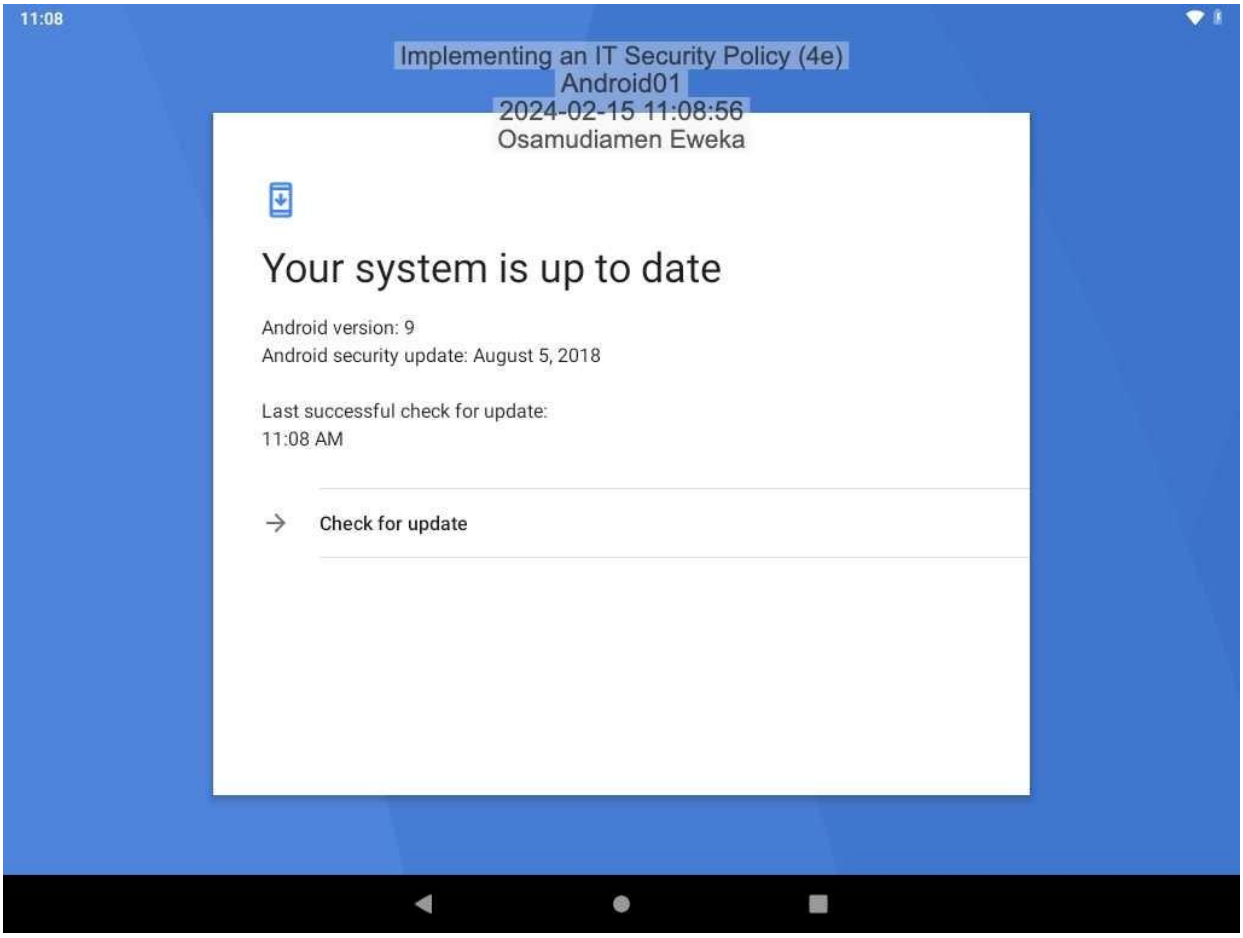
Participants then move to the Security Status section to access Security Update settings via the Security Update option. Here, the "Check for Update" command is used to query Google's servers for the latest security patch. Despite a potential message indicating that the system is up to date, it's important to note that for Android Version 9, Google provided security patch support until Fall 2021, with the last update in August 2018 (Android OS, 2024). This highlights the limitations of virtualized mobile systems but also underscores the importance of regular security maintenance. The process emphasizes the essential practice of always updating

to the latest security patches, despite the possible initial bugs in major OS updates, to protect against vulnerabilities.

Additionally, participants are to document the process by capturing a screenshot of the "last successful check for update" timestamp as shown in Figure 10 below (Jones & Bartlett, 2024). This step serves as a practical demonstration of the update procedure, providing tangible evidence of the device's current security status and ensuring that the latest security measures have been applied effectively.

Figure 10

Make a screen capture showing the updated "last successful check for update" timestamp.



Next Within the Device Security framework, the participant navigates to the Screen Lock settings by selecting the "Screen Lock" option. This action leads to an interface where various screen lock mechanisms are presented, ranging from minimal security options such as None and Swipe, to more secure alternatives like Pattern, PIN, and Password. The document highlights that while biometric features like fingerprint and facial recognition offer advanced security, they may not be inherently superior to traditional methods due to potential coercion risks. The discourse advocates for multifactor authentication as a balanced approach between security and usability.

The participants is then instructed to enhance the device's security by opting for a Password screen lock, a method deemed more secure than the device's existing settings. This choice is facilitated through a selection on the "Choose screen lock" page, leading to the "Set screen lock" page where the password P@ssw0rd! is inputted, followed by a verification step requiring the password's re-entry.

Subsequent steps involve adjusting notification settings to hide sensitive content, reinforcing privacy. The process culminates in a system reboot through the "Power Cycle" feature on the Lab View toolbar to initialize the updated security configurations.

The narrative concludes with an instruction to document the updated Android lock screen via screen capture, serving as empirical evidence of the security enhancement Figure 11 illustrates this screen capture (Jones & Bartlett, 2024). This stepwise elucidation encapsulates the procedural methodology for augmenting device security through the implementation of a password-based screen lock, underscored by a scholarly examination of the comparative security merits of various locking mechanisms.

Figure 11

Make a screen capture showing the Android lock screen.

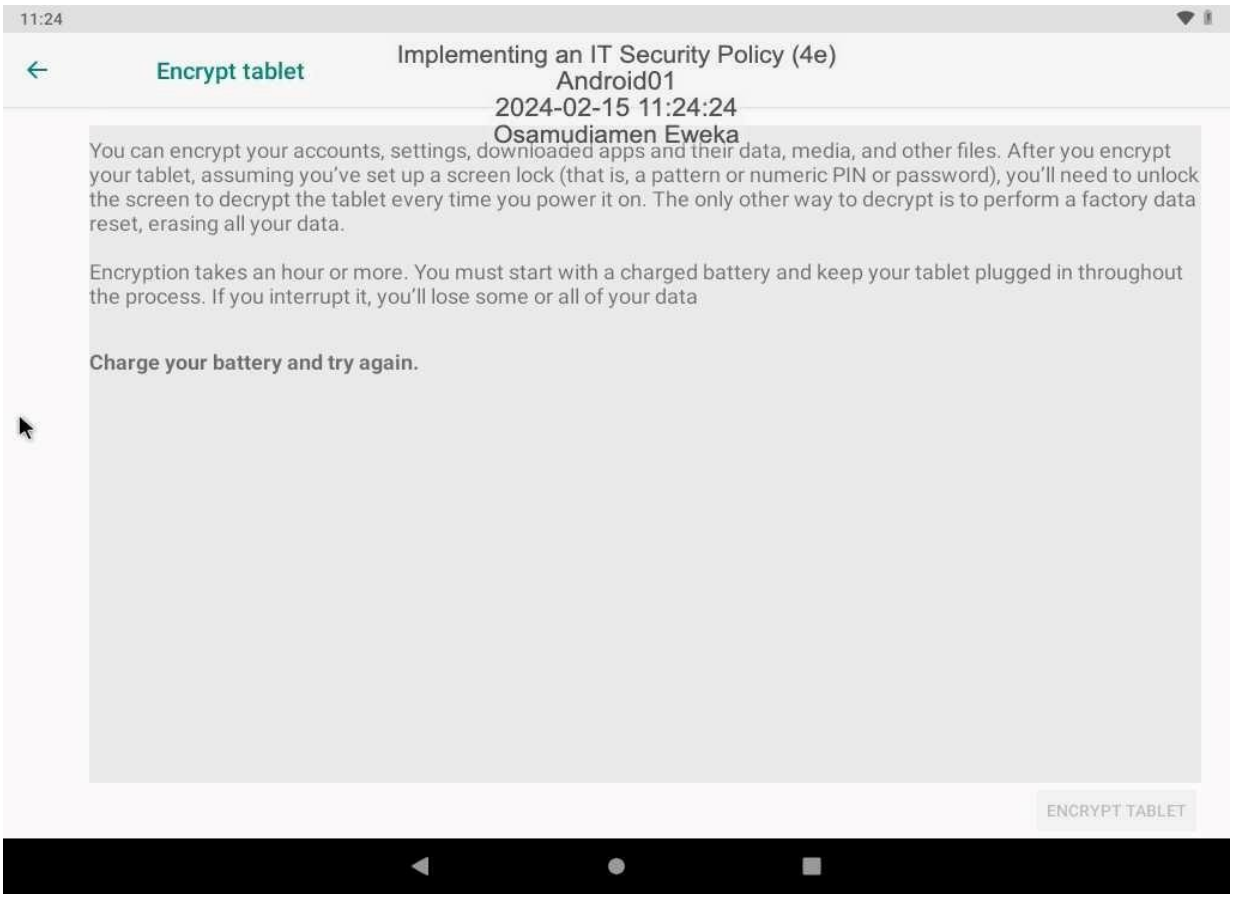
To finalize the security enhancements on the Android01 device, the aims to activate device encryption and the Find My Device feature. This involves navigating from the home screen to the Security & location settings, then accessing the Encryption & credentials section to select "Encrypt tablet." However, due to the virtual environment's limitations, a prompt appears advising to charge the device before proceeding, highlighting a common hurdle in virtual setups.

Despite this, the prompt underscores encryption's importance as a top-tier security measure to protect data from unauthorized access, while acknowledging that highly skilled entities might still breach it with advanced tools.

The participants are advised to take a screenshot of this encryption setup explanation, capturing the essence of attempting to enhance the device's security and illustrating the critical role encryption plays in safeguarding mobile data as shown below in Figure 12 (Jones & Bartlett, 2024).

Figure 12

Make a screen capture showing the encryption set-up explanation.



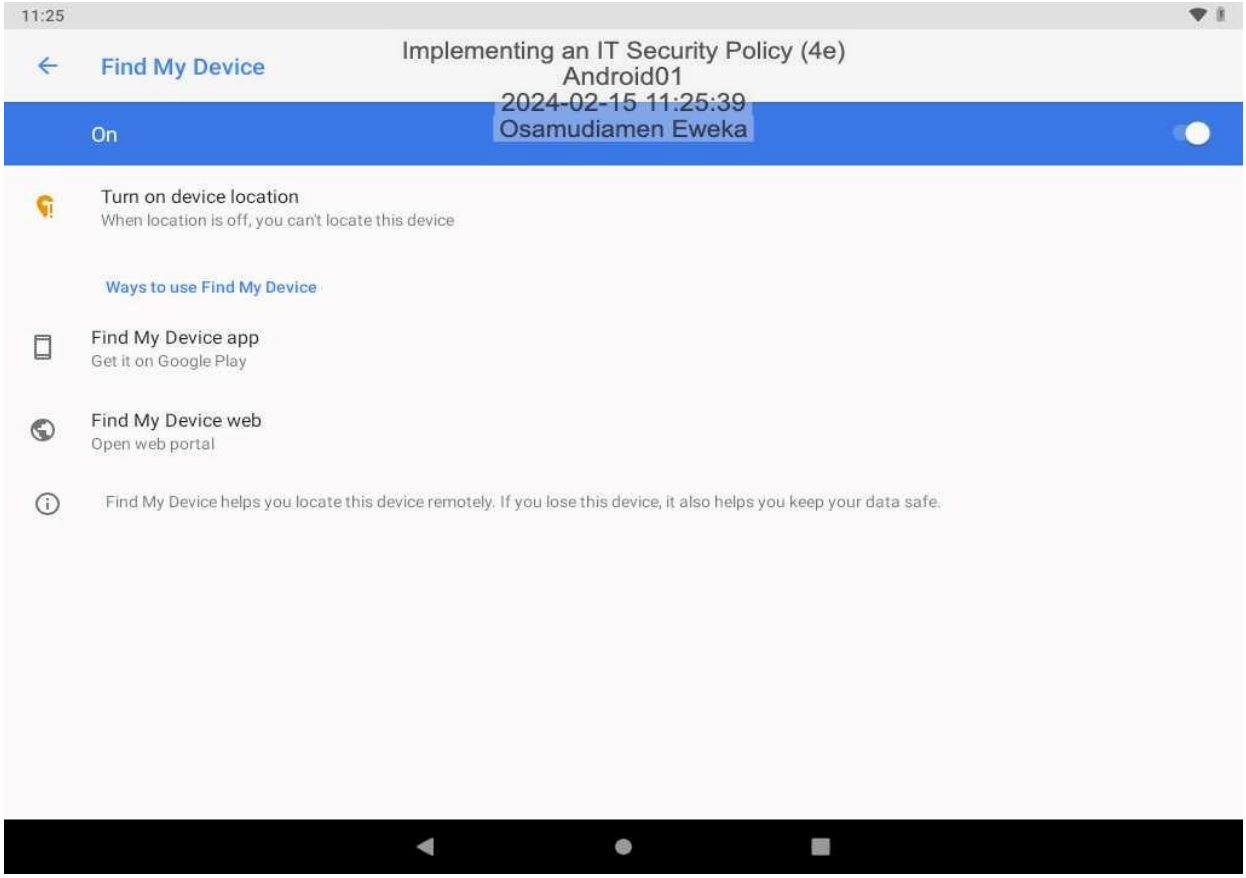
After revisiting the Security & location settings on the Android01 device, the participant selects the Find My Device option, intending to enhance the device's security further. However, due to the constraints of operating within a virtualized environment, activating this feature is not possible.

Find My Device, known in some contexts as Android Device Manager, is a critical security tool on actual Android devices, offering capabilities to remotely track, lock, and erase the device. This function is particularly valuable in situations where a device is lost or stolen, providing a layer of security to prevent unauthorized access to sensitive information.

Next participants are to document the attempt to activate Find My Device by capturing a screenshot of the settings page shown in Figure 13 (Jones & Bartlett, 2024). This action underscores the importance of such features in protecting personal and professional data on mobile devices, illustrating the proactive steps taken towards comprehensive device security.

Figure 13

Make a screen capture showing the Find My Device settings.



Section 3: Result and Analysis

Part 1: Research Acceptable Use Policies

Using the Internet, **research** Acceptable Use Policies, then **identify** at least five common policy statements and **explain** their significance. Be sure to cite your sources.

The five different policies are as follows:

1. Prohibited activities: Common policy statements prohibit certain activities such as unauthorized access, hacking, spamming, and the distribution of illegal or harmful content. These activities are usually illegal and can damage the company's reputation, pose security risks and be a source of liability (Bika, 2023).
2. Usage restrictions: Acceptable Use Policies often restrict the use of company resources, such as computers and internet access, to work-related activities. Personal use may be permitted, but only during non-working hours and in accordance with the policy (Bika, 2023).
3. Confidentiality and data protection: Confidential information such as company data, client data, and employee data should be kept confidential and protected in accordance with the policy. This includes restrictions on sharing, copying, and storing confidential information on personal devices (Kelly, 2020).
4. Monitoring: Companies may monitor the use of their resources, including email, internet access, and computer usage, to ensure compliance with the policy and to prevent any prohibited (Kelly, 2020).
5. activities. This can be important for ensuring the security of company data and for investigating any potential policy violations (Kelly, 2020).

6. Consequences of violation: Acceptable Use Policies typically outline the consequences for violating the policy, including disciplinary action, termination, and potentially legal action. This helps to establish clear expectations for employees and to ensure that the policy is taken seriously (Kelly, 2020).

Explanation:

In conclusion, Acceptable Use Policies are important for ensuring the proper use of company resources and protecting confidential information, data and the company's reputation. These policies typically outline prohibited activities, usage restrictions, confidentiality and data protection measures, monitoring practices, and the consequences of policy violations. It is important to follow contemporary best practices and regularly review and update the policy to keep it relevant and effective.

Section 3: Result and Analysis

Part 2: Research Privacy Policies

Using the Internet, research user Privacy Policies, then identify at least five common policy statements and explain their significance. Be sure to cite your sources.

The user privacy policy are as follows:

1. Collection of Personal Information: Privacy policies often specify the type of personal information that is collected, the purpose for collecting it, and how it will be used. This helps to build trust with users by being transparent about the data that is collected and how it will be used (Usercentrics, 2023).
2. Data Security: Privacy policies typically include statements about the measures taken to secure personal information, such as encryption and secure storage. This helps to protect users' personal information from unauthorized access and breaches (Usercentrics, 2023).
3. Data Sharing: Privacy policies often outline the circumstances under which personal information may be shared with third parties, such as for legal reasons or to provide services. This helps users to understand when their personal information may be shared and who it may be shared with (Juang, 2023).
4. Data Retention: Privacy policies often specify how long personal information will be retained and when it will be deleted. This helps to ensure that personal information is not kept for longer than necessary and to manage the risk of data breaches (Juang, 2023).
5. User Control: Privacy policies may give users control over their personal information, such as the ability to access, correct, or delete their information. This helps to empower users and give them greater control over their personal information (Juang, 2023).

Explanation:

In conclusion, Privacy Policies play an important role in protecting the personal information of users and building trust with them. They typically outline the type of personal information collected, measures taken to secure it, circumstances for sharing it with third parties, data retention policies, and user control over their personal information. It is important to follow contemporary best practices and regularly review and update the policy to ensure it remains relevant and effective.

Conclusion

The lab work on implementing an IT Security Policy focused on practical applications of security measures in IT environments, including password protection, antivirus policy implementation, applying Windows security baselines, and mobile device security. The lab also delved into theoretical aspects like researching Acceptable Use Policies and Privacy Policies, emphasizing their importance in safeguarding company resources, data, and reputation, as well as in protecting user privacy. The conclusion drawn highlighted the critical role of such policies in ensuring proper resource usage, confidentiality, data protection, and establishing clear guidelines and consequences for violations, alongside the importance of regular review and updates to stay effective and relevant.

Reference

Android OS. (2024, January 8). end-of-life. Date. https://endoflife.date/android

Bika, N. (2023, September 26). *The 5 company policies you need to have in writing*. Recruiting Resources: How to Recruit and Hire Better. https://resources.workable.com/tutorial/the-5-company-policies-you-need-to-have-in-writing

Habte, F. (2021, October 19). *What is an IT Security Policy?* Check Point Software. https://www.checkpoint.com/cyber-hub/cyber-security/what-is-it-security/it-security-policy/

Jones & Bartlett (2024). Applying User Authentication and Access Controls (Figures). *Jones and BartlettLearning Virtual Lab*. URL: https://jbl-lti.hatsize.com/startlab

Juang, R. (2023, December 8). What is a privacy policy? Ironclad. https://ironcladapp.com/journal/contracts/how-to-create-the-best-privacy-policy-for-your-business/#:~:text=A%20privacy%20policy%20is%20a,protect%20both%20company%20and%20consumers.

Kelly, M. (2020, September 24). *Why it's important to have policies and procedures: 4 reasons*. GAN Integrity. https://www.ganintegrity.com/blog/why-its-important-to-have-policies-and-procedures/#:~:text=Another%20way%20to%20phrase%20it,handle%20a%20customer%20service%20call.

Usercentrics. (2023, December 18). *What is a privacy policy and why do you need one?* Consent Management Platform (CMP) Usercentrics. https://usercentrics.com/knowledge-hub/what-is-a-privacy-policy-and-why-do-you-need-

one/#:~:text=A%20privacy%20policy%20is%20a,with%20respect%20to%20their%20data.