Student:	Email:
Fernando Parra	fparra1@msudenve.edu

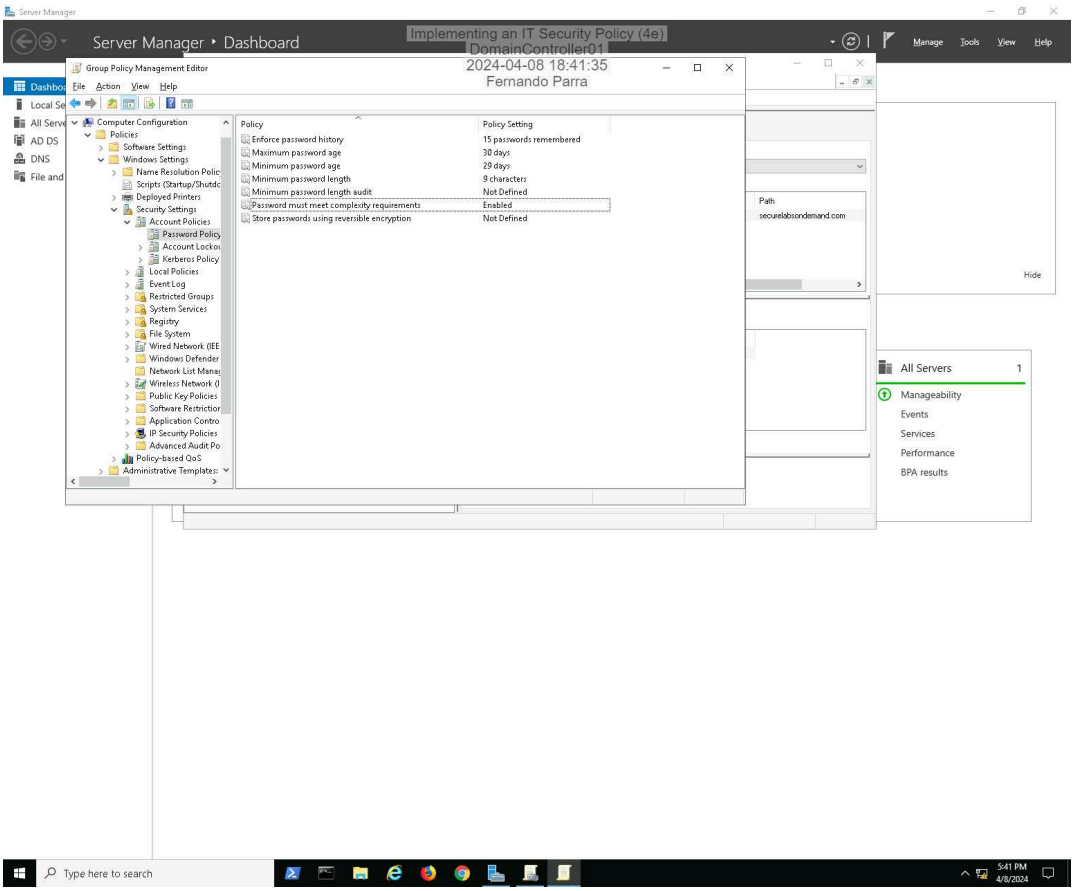
Time on Task:	Progress:
4 hours, 54 minutes	100%

Report Generated: Monday, April 8, 2024 at 10:52 PM

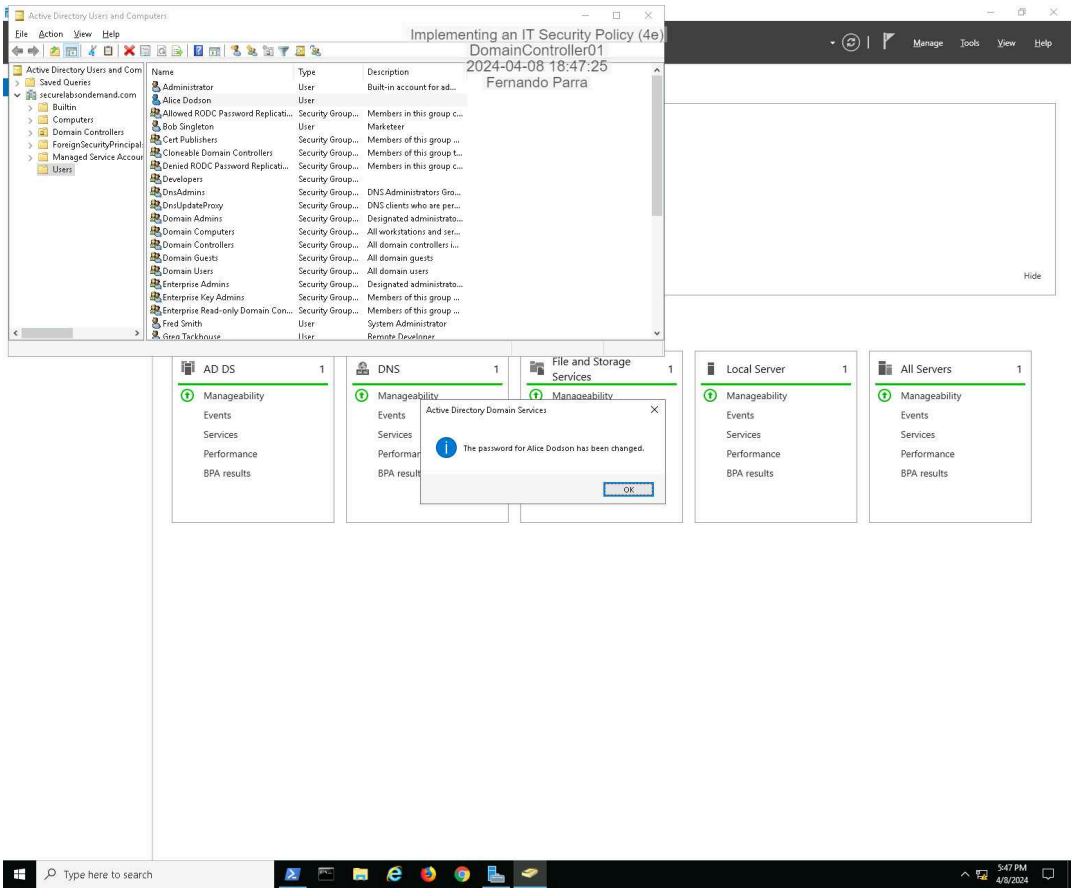
Section 1: Hands-On Demonstration

Part 1: Implement a Password Protection Policy

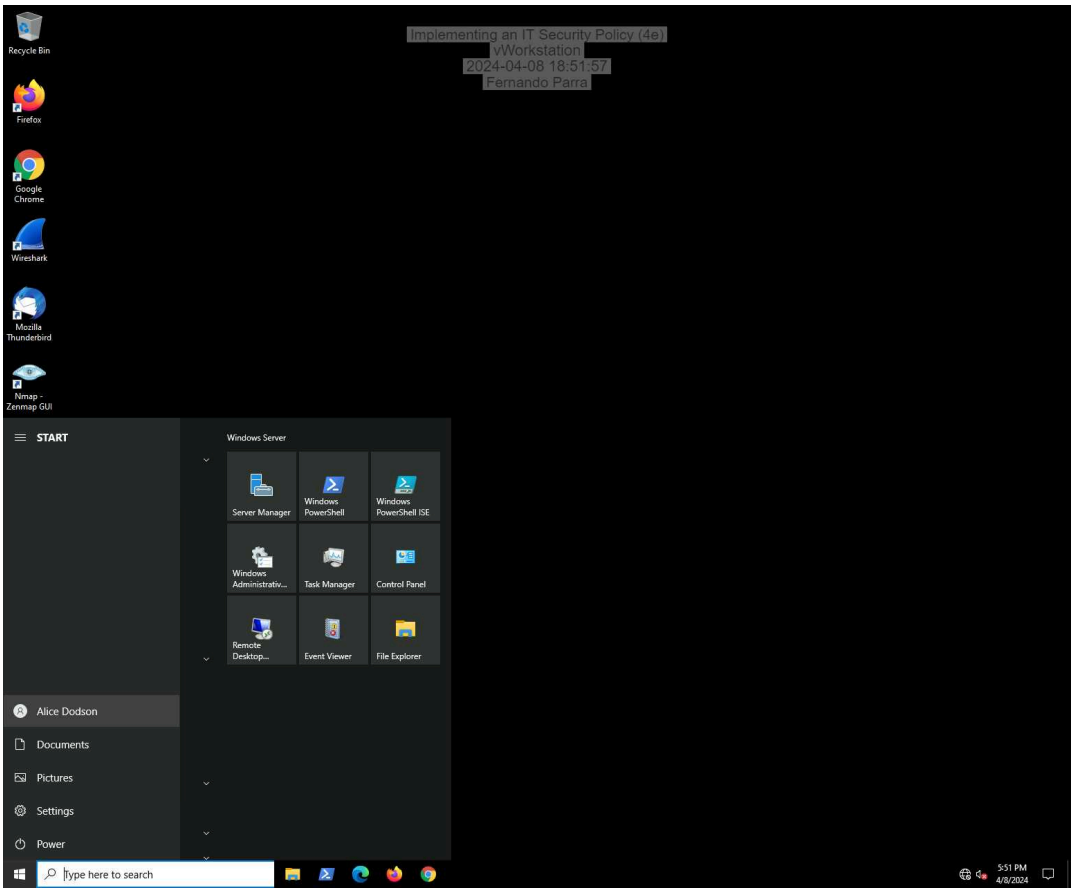
16. **Make a screen capture** showing the **newly configured Domain Password Policy settings**.



28. **Make a screen capture** showing the **successful password change message**.

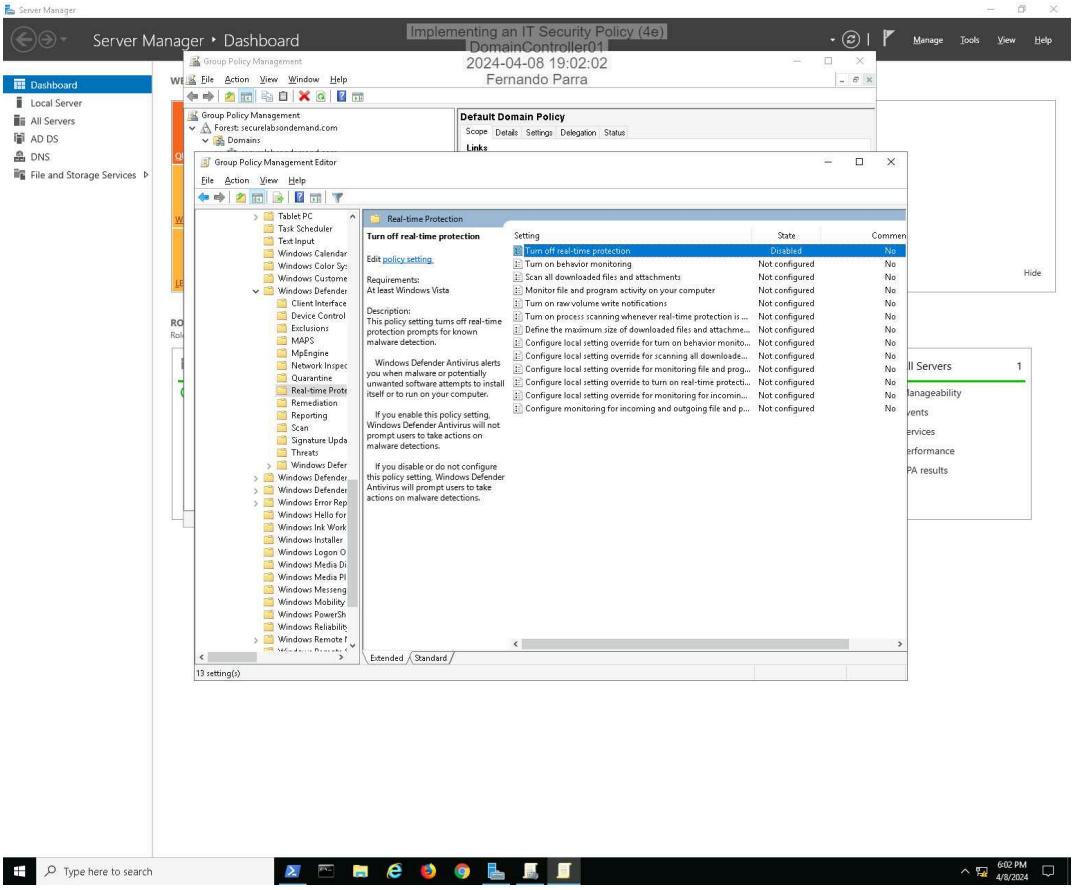


36. **Make a screen capture** showing the **logged on user account**.

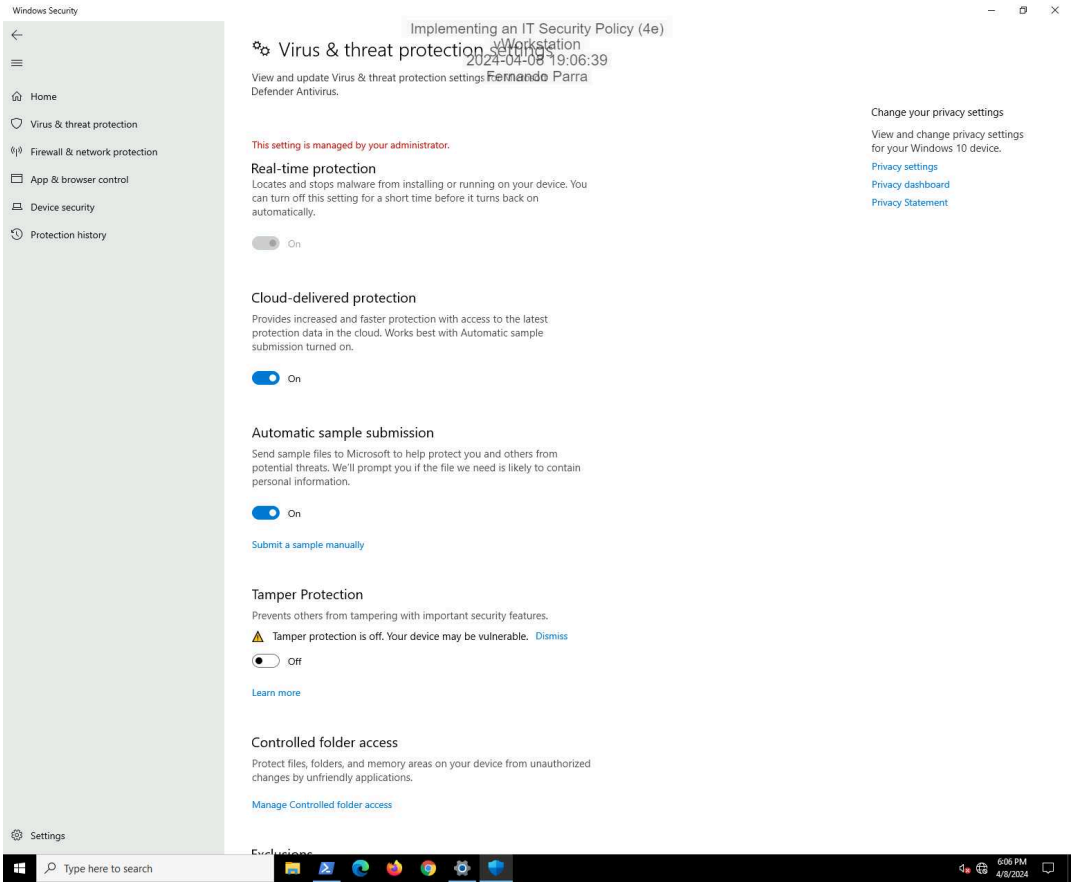


Part 2: Implement an Antivirus Policy

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



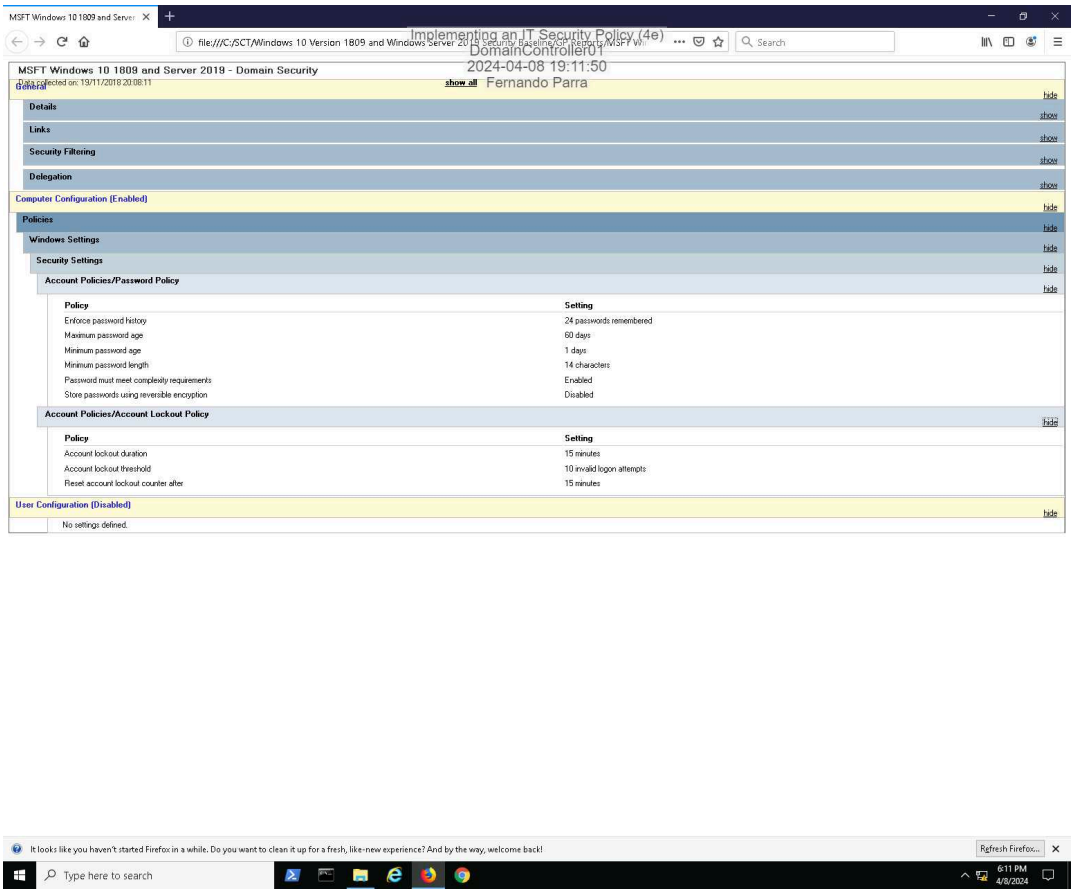
25. **Make a screen capture** showing the **grayed-out real-time threat protection settings**.



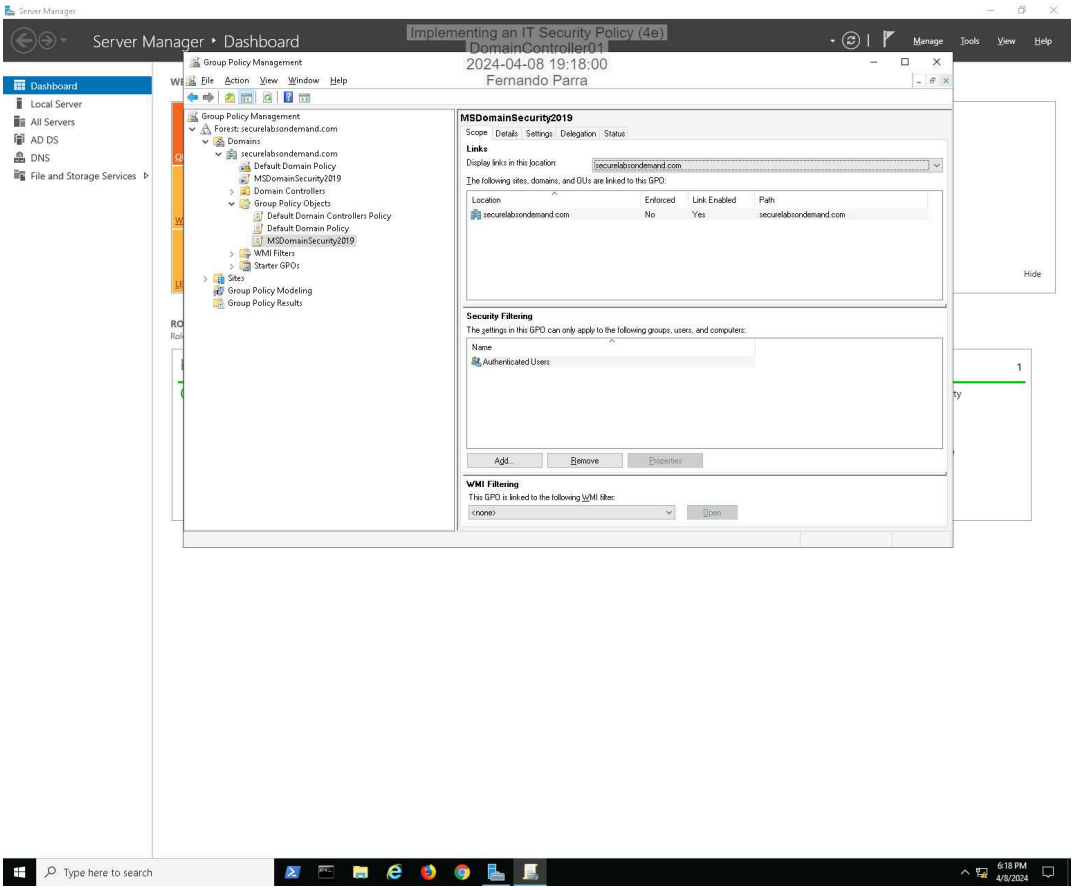
Section 2: Applied Learning

Part 1: Apply a Windows Security Baseline

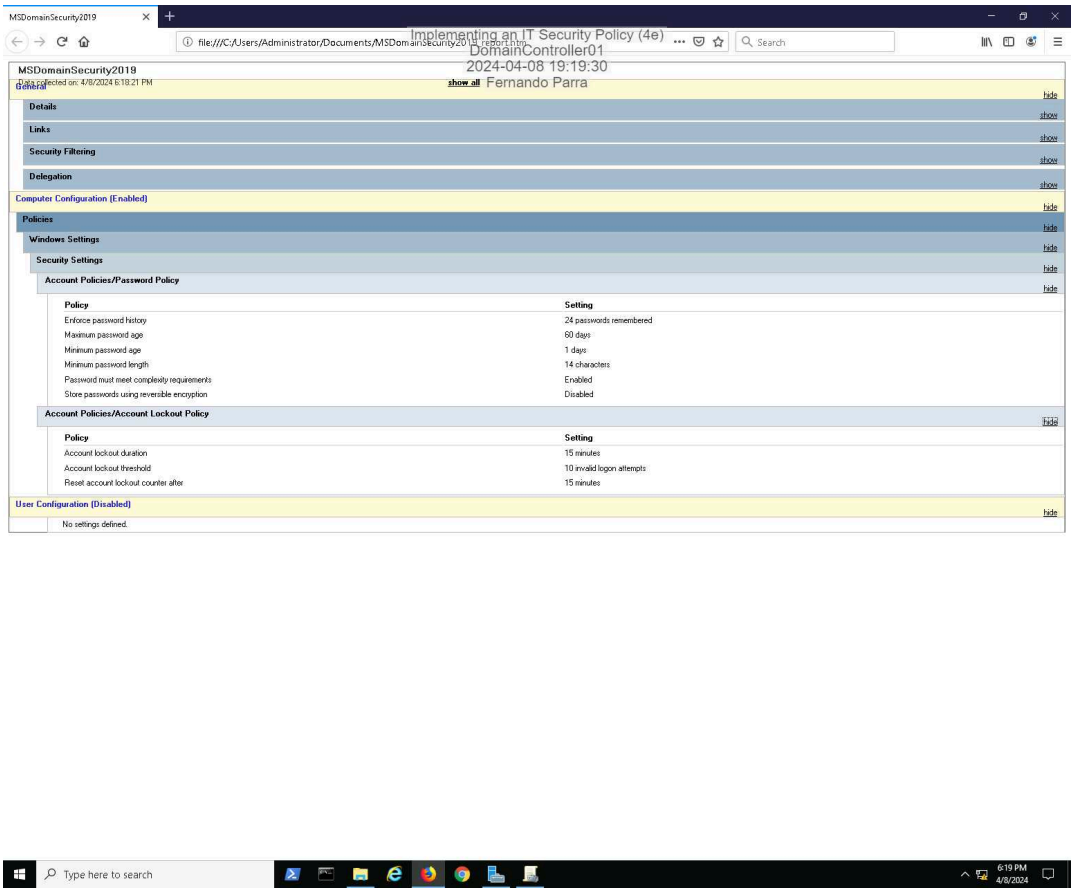
6. **Make a screen capture** showing **Microsoft's recommended Password and Account Lockout policy settings**.



19. **Make a screen capture** showing the **linked MSDomainSecurity2019 object**.

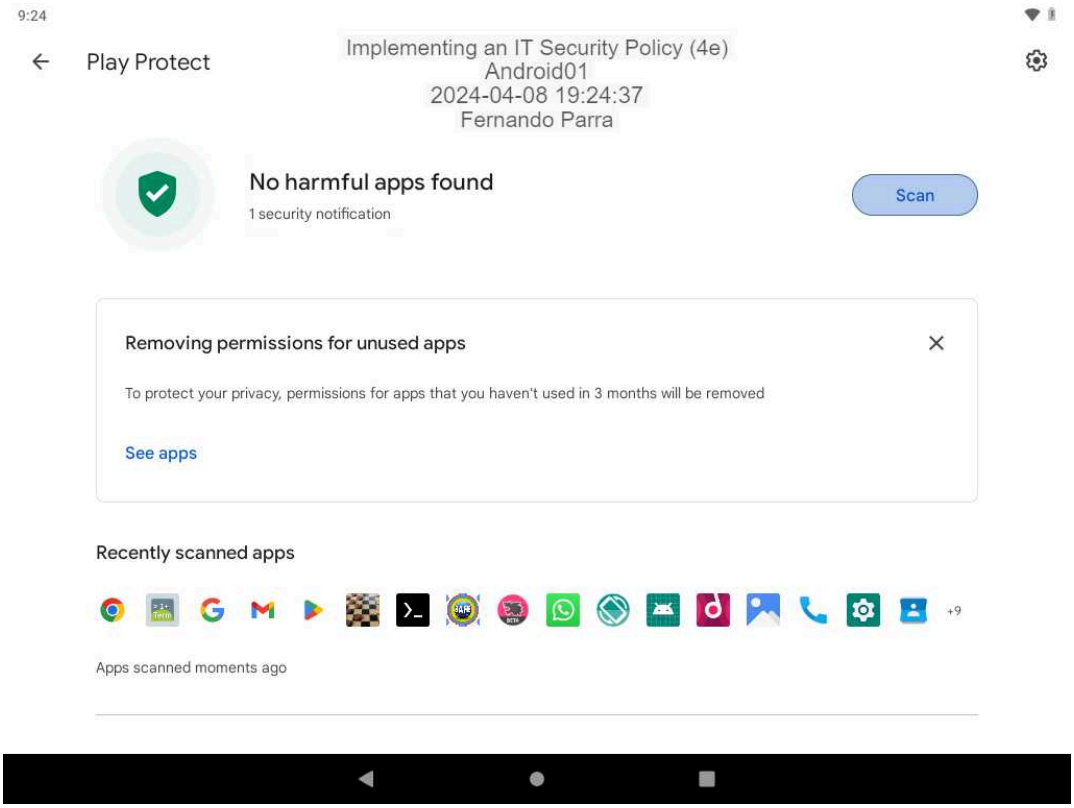


23. **Make a screen capture** showing the **Password and Account Lockout policy settings**.

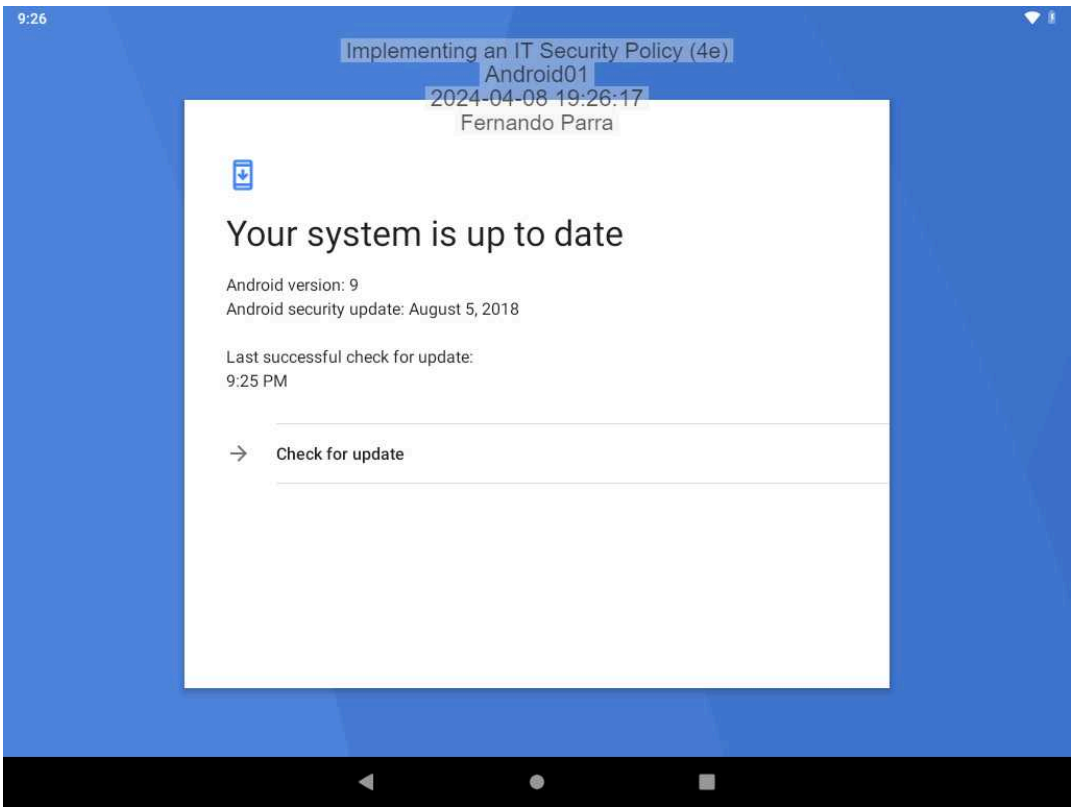


Part 2: Implement a Mobile Device Security Policy

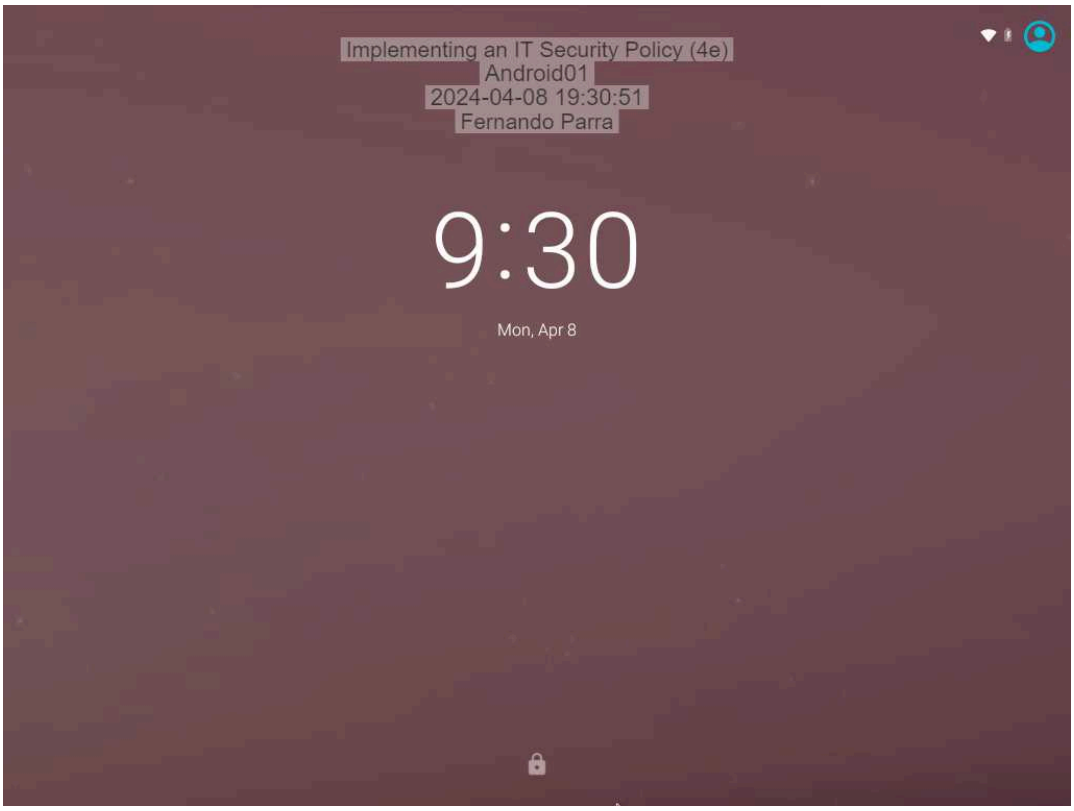
7. **Make a screen capture** showing the **results of the Google Play Protect scan**.



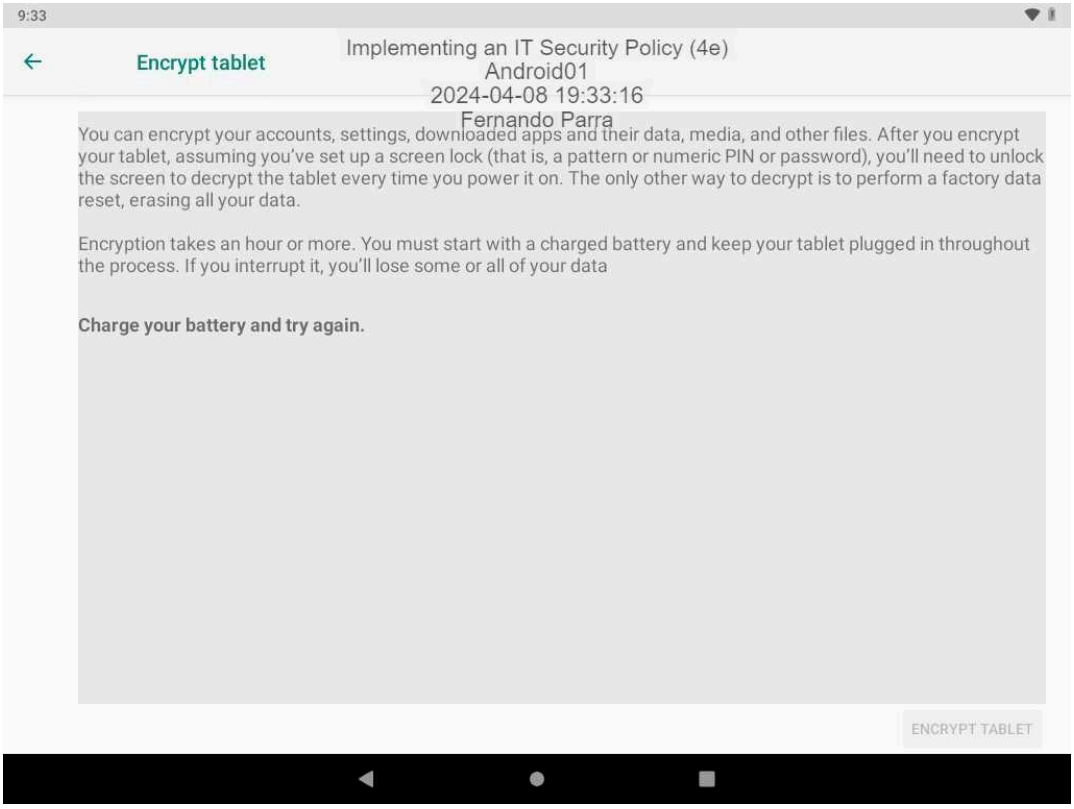
11. **Make a screen capture** showing the **updated "last successful check for update" timestamp**.



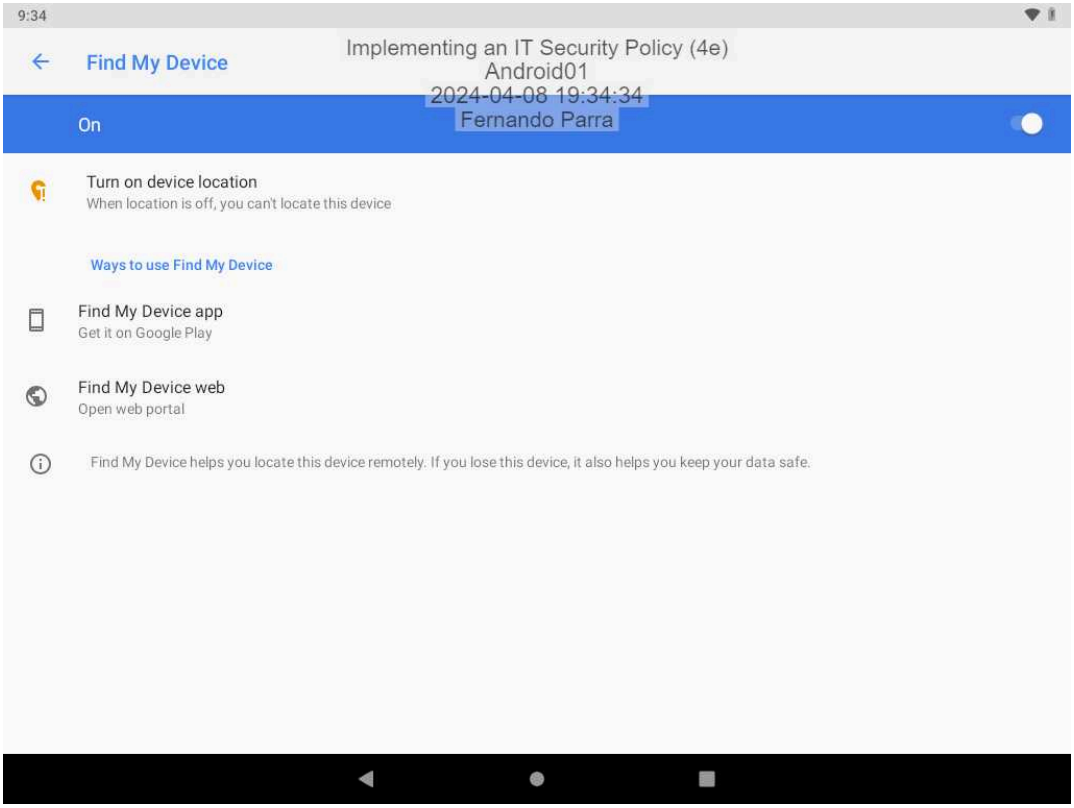
19. **Make a screen capture** showing the **Android lock screen**.



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



27. **Make a screen capture** showing the **Find My Device settings**.



Section 3: Challenge 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.

Passwords: passwords cannot be easily guessed, passwords must be complex, consisting of at least 12 characters, including a mix of uppercase and lowercase letters, numbers, and special characters. Users are restricted from employing easily guessed information such as personal names, birthdates, or common words. In addition, users also have to change their passwords every 30-90 days, preferably within 30 days. Failure to comply with the following requirements may result in an account breach and compromise confidential data.
Privacy and Confidentiality: users should handle information, such as employee data or trade secrets of Secure Labs On Demand confidential. This covers how users can access, store, and transmit sensitive information as well as the importance of keeping their personal information secure and not sharing it with unauthorized individuals. Failure to protect confidential information can lead the company to reputational damage, legal action, and financial losses.
Illegal Activities: the prohibition of unlawful activities forbids users from engaging in any action that is deemed unlawful, such as hacking, distributing malware, spam, phishing, viruses, worms, copyright infringement, etc. This protects Secure Labs On Demand from risk, safeguards data, and maintains the security and integrity of the network ensuring a safe environment for all users of Secure Labs On Demand.
Intellectual Property: This specifies users' relation with the intellectual property rights of Secure Labs On Demand and prohibits the use of copyrighted material, trademarks, or trade secrets without permission. Unauthorized use of copyrighted materials can result in legal action and financial consequences for both the user and Secure Labs On Demand, it also ensures that Secure Labs On Demand and individuals are fairly compensated for their work.
Software: Using approved software to ensure the security and integrity of our digital environment is enforced, unauthorized or unapproved software can present vulnerabilities and raise the risk of malware infections, data breaches, and system malfunctions hence users are prohibited from installing unapproved software without prior authorization. Adhering to approved software protects Secure Labs On Demand data, reduces security vulnerabilities, and ensures that all software is up-to-date with the latest security patches and features.
References
https://www.utc.edu/information-technology/information-security/acceptable-use-policy
https://www.ndu.edu/Portals/59/Documents/Incoming/AY24/NDU%20Acceptable%20Use%20Policy%20(AUP).pdf?ver=2K9ZhQRQNb1jZtHd5W5afQ%3D%3D
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-47r1.pdf
https://www.comptia.org/blog/security-awareness-training-corporate-acceptable-use-policy

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.

Collection of Data: Secure Labs On Demand will collect personal information only when necessary to provide services and improve experience. Secure Labs On Demand may collect contact information, payment details, and usage data for internal record keeping and to communicate with you about our products and services.
Sharing and Disclosure of Data: Secure Labs On Demand does not sell, rent, or lease personal information to third parties without consent, except as required by law. Secure Labs On Demand may share personal information with affiliates or partners to provide jointly offered services or to complete transactions initiated by the user.
Security and Protection of Data: Secure Labs On Demand implements physical, digital, and administrative measures to protect and secure the personal information collected. Access to personal data is restricted to authorized personnel only, and security policies and procedures to ensure they are up-to-date and effective are implemented through professional third-party auditing services.
Data Storage and Access: Secure Labs On Demand retains personal information only for as long as necessary to provide services or as required by law. Users have the right to access, update, or delete personal information at any time. Users may also request a copy of the data we hold about you in a commonly used, machine-readable format.
Other Technologies: Secure Labs On Demand uses cookies and other technologies to provide customized services and enhance user experience. Secure Labs On Demand may use these tools to collect usage data, including browser type, operating system, and IP address. Users can control the use of cookies through web browser settings. By using Secure Labs On Demand services, users consent to the use of cookies and other technologies under the user privacy policy.
References
https://www.linkedin.com/legal/privacy-policy
https://www.linkedin.com/pulse/privacy-policy-importance-purpose-drafting-tips-pakhi-garg
https://cybersecurityguide.org/privacy-policy/