Implementing an IT Security Policy (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 07

Student:	Email:
Mustafa Shah	ho3168@wayne.edu

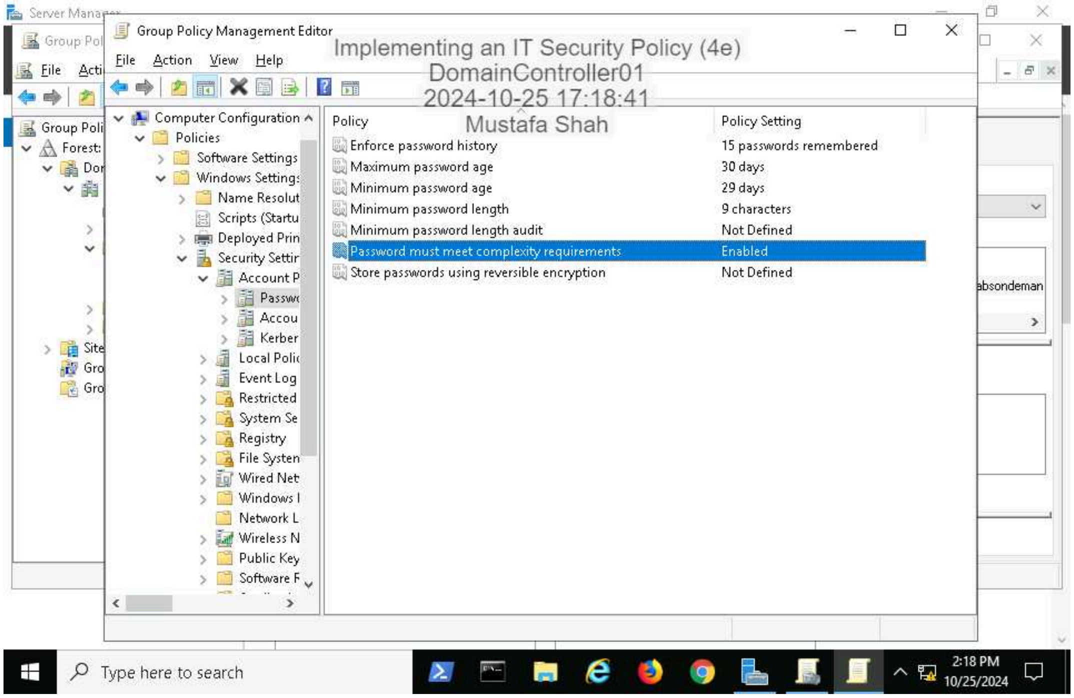
Time on Task:	Progress:
0 hours, 56 minutes	100%

Report Generated: Friday, October 25, 2024 at 5:58 PM

Section 1: Hands-On Demonstration

Part 1: Implement a Password Protection Policy

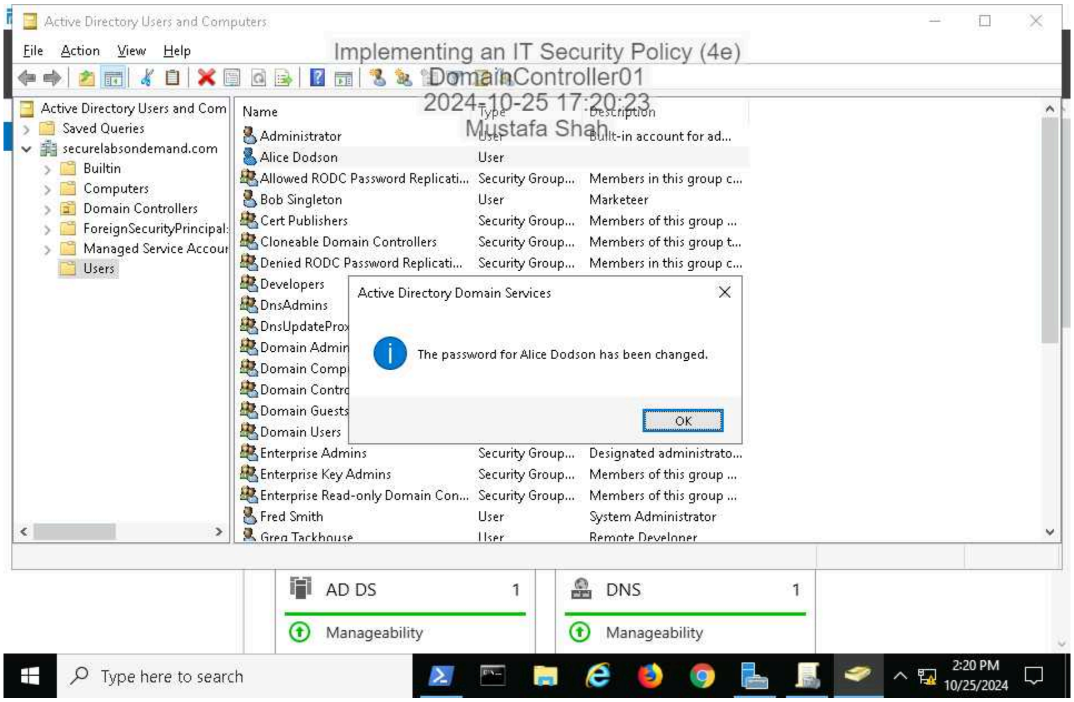
16. **Make a screen capture** showing the **newly configured Domain Password Policy settings**.



Implementing an IT Security Policy (4e)
DomainController01
2024-10-25 17:18:41
Mustafa Shah

Policy	Policy Setting
Enforce password history	15 passwords remembered
Maximum password age	30 days
Minimum password age	29 days
Minimum password length	9 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Not Defined

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



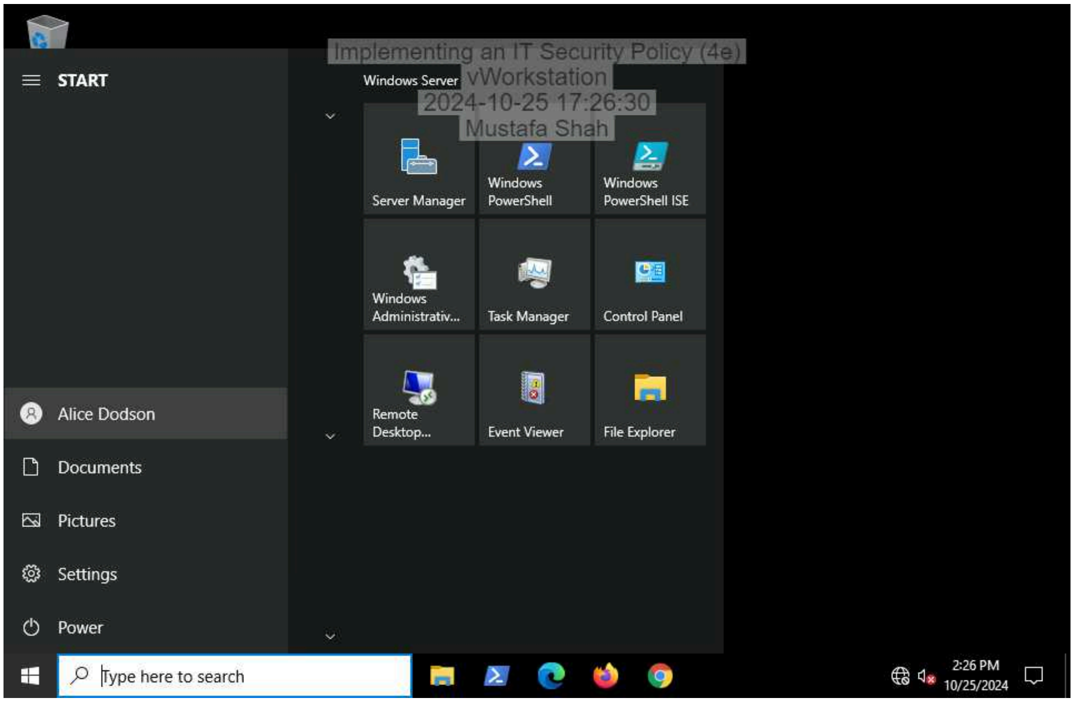
Name	Type	Description
Administrator	User	Built-in account for ad...
Alice Dodson	User	
Allowed RODC Password Replicati...	Security Group...	Members in this group c...
Bob Singleton	User	Marketeer
Cert Publishers	Security Group...	Members of this group ...
Cloneable Domain Controllers	Security Group...	Members of this group t...
Denied RODC Password Replicati...	Security Group...	Members in this group c...
Developers		
DnsAdmins		
DnsUpdateProx		
Domain Admin		
Domain Comp		
Domain Contro		
Domain Guests		
Domain Users		
Enterprise Admins	Security Group...	Designated administrato...
Enterprise Key Admins	Security Group...	Members of this group ...
Enterprise Read-only Domain Con...	Security Group...	Members of this group ...
Fred Smith	User	System Administrator
Greg Tackhouse	User	Remote Developer

Active Directory Domain Services

The password for Alice Dodson has been changed.

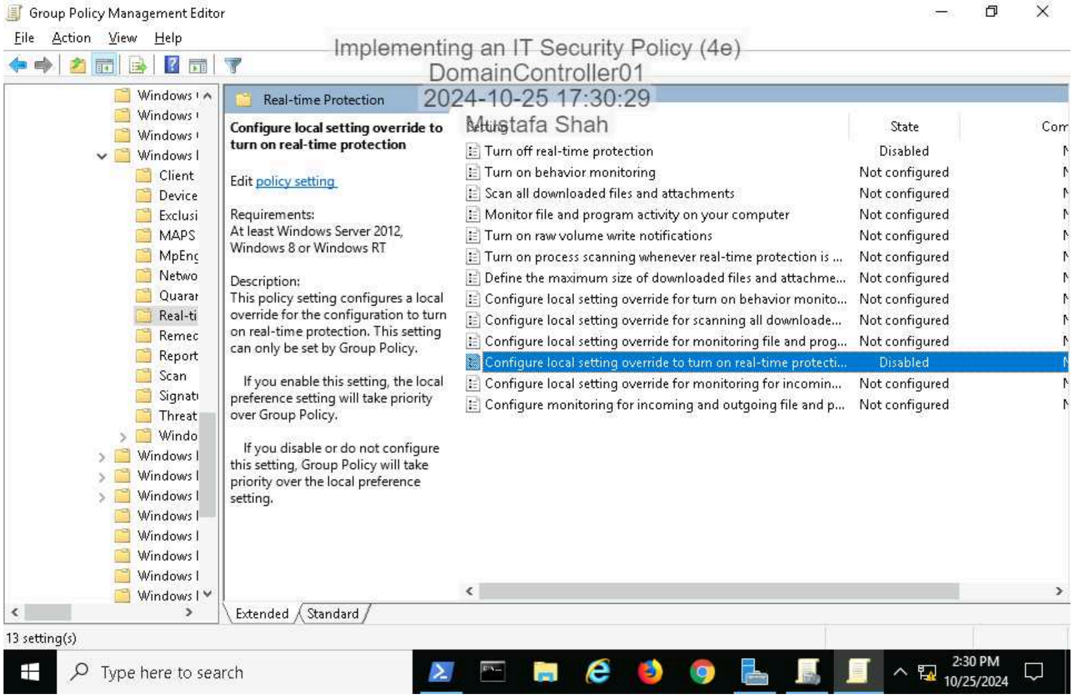
OK

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.**



Implementing an IT Security Policy (4e)
DomainController01
2024-10-25 17:30:29
Mustafa Shah

Real-time Protection

Configure local setting override to turn on real-time protection

Edit policy setting

Requirements:
At least Windows Server 2012, Windows 8 or Windows RT

Description:
This policy setting configures a local override for the configuration to turn on real-time protection. This setting can only be set by Group Policy.

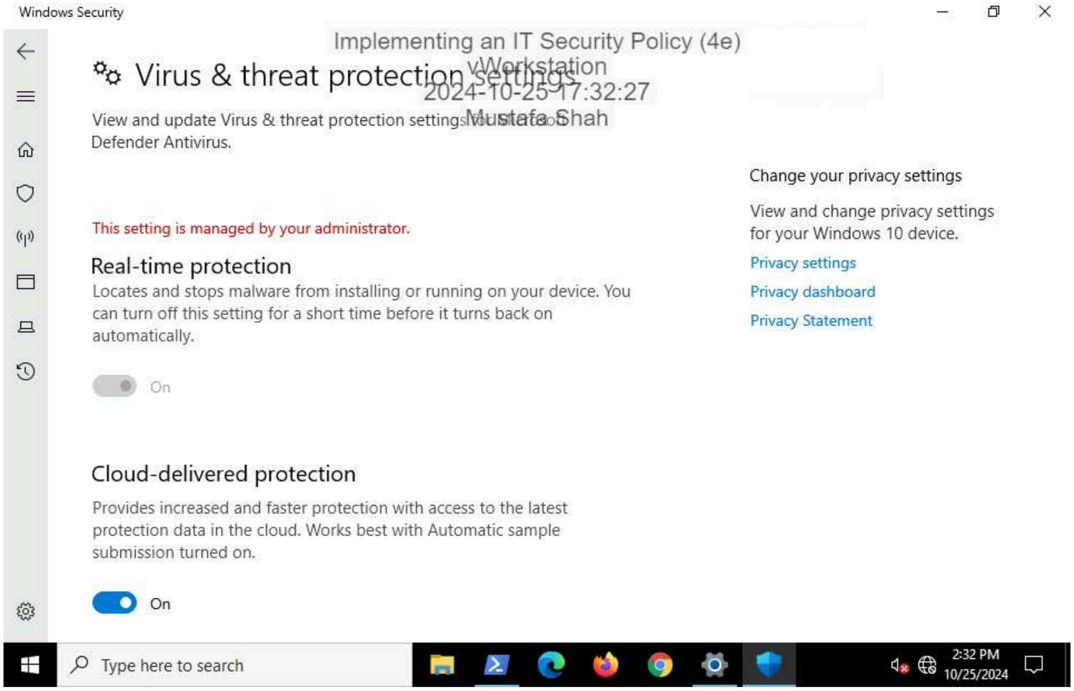
If you enable this setting, the local preference setting will take priority over Group Policy.

If you disable or do not configure this setting, Group Policy will take priority over the local preference setting.

Setting	State	Com
Turn off real-time protection	Disabled	N
Turn on behavior monitoring	Not configured	N
Scan all downloaded files and attachments	Not configured	N
Monitor file and program activity on your computer	Not configured	N
Turn on raw volume write notifications	Not configured	N
Turn on process scanning whenever real-time protection is ...	Not configured	N
Define the maximum size of downloaded files and attachme...	Not configured	N
Configure local setting override for turn on behavior monito...	Not configured	N
Configure local setting override for scanning all downloade...	Not configured	N
Configure local setting override for monitoring file and prog...	Not configured	N
Configure local setting override to turn on real-time protecti...	Disabled	N
Configure local setting override for monitoring for incomin...	Not configured	N
Configure monitoring for incoming and outgoing file and p...	Not configured	N

13 setting(s)

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



Implementing an IT Security Policy (4e)
vWorkstation
2024-10-25 17:32:27
Mustafa Shah

Virus & threat protection settings

View and update Virus & threat protection settings for Microsoft Defender Antivirus.

This setting is managed by your administrator.

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

On

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

On

Change your privacy settings

View and change privacy settings for your Windows 10 device.

Privacy settings

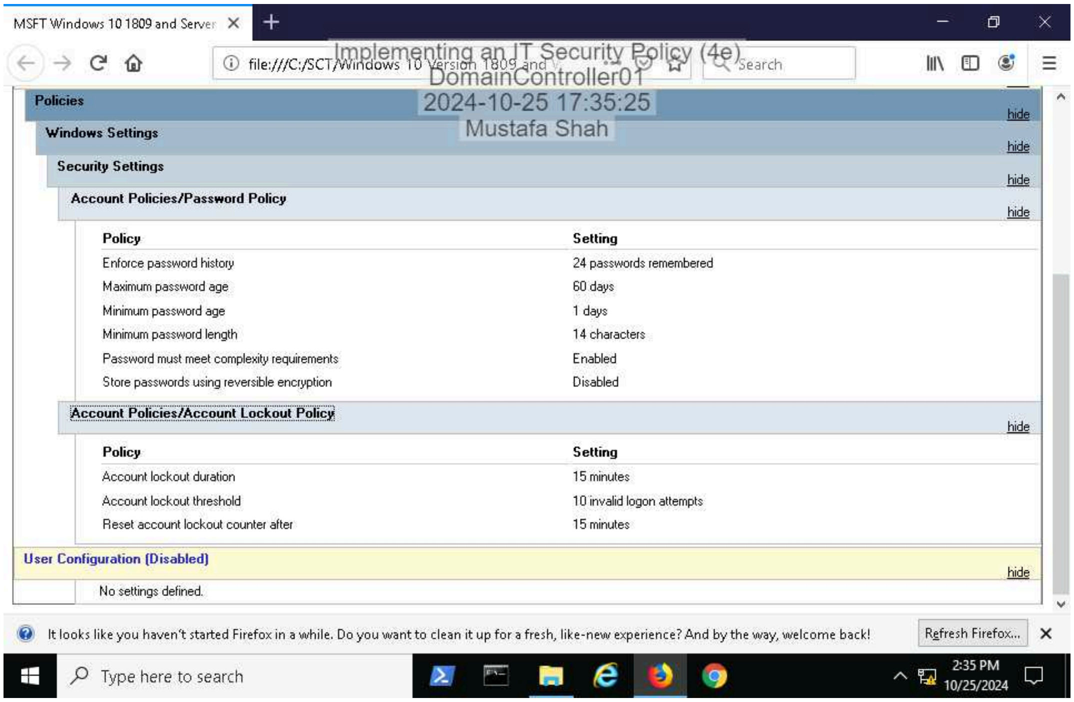
Privacy dashboard

Privacy Statement

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**.


MSFT Windows 10 1809 and Server
file:///C:/SCT/Windows 10 Version 1809 and
Search
hide
Refresh Firefox...
Type here to search
2:35 PM
10/25/2024

Implementing an IT Security Policy (4e)
DomainController01
2024-10-25 17:35:25
Mustafa Shah

Policies

Windows Settings

Security Settings

Account Policies/Password Policy

Policy	Setting
Enforce password history	24 passwords remembered
Maximum password age	60 days
Minimum password age	1 days
Minimum password length	14 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Account Policies/Account Lockout Policy

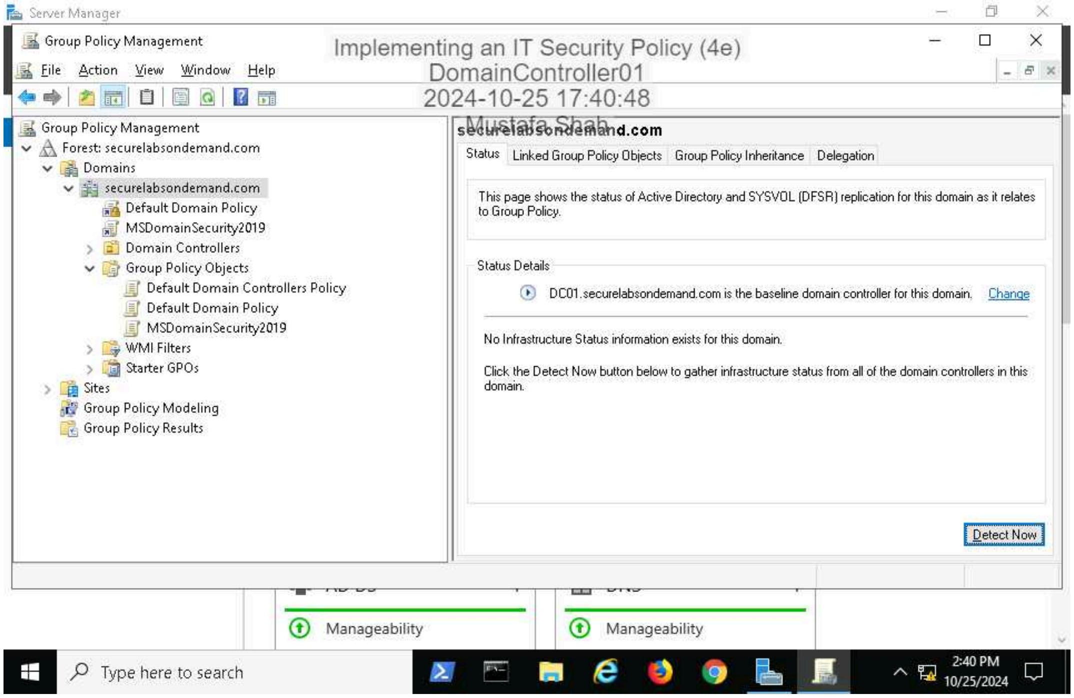
Policy	Setting
Account lockout duration	15 minutes
Account lockout threshold	10 invalid logon attempts
Reset account lockout counter after	15 minutes

User Configuration (Disabled)

No settings defined.

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

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



- Group Policy Management
  - Forest: securelabsondemand.com
    - Domains
      - securelabsondemand.com
        - Default Domain Policy
        - MSDomainSecurity2019
        - Domain Controllers
        - Group Policy Objects
          - Default Domain Controllers Policy
          - Default Domain Policy
          - MSDomainSecurity2019
        - WMI Filters
        - Starter GPOs
    - Sites
    - Group Policy Modeling
    - Group Policy Results

securelabsondemand.com

Status | Linked Group Policy Objects | Group Policy Inheritance | Delegation

This page shows the status of Active Directory and SYSVOL (DFSR) replication for this domain as it relates to Group Policy.

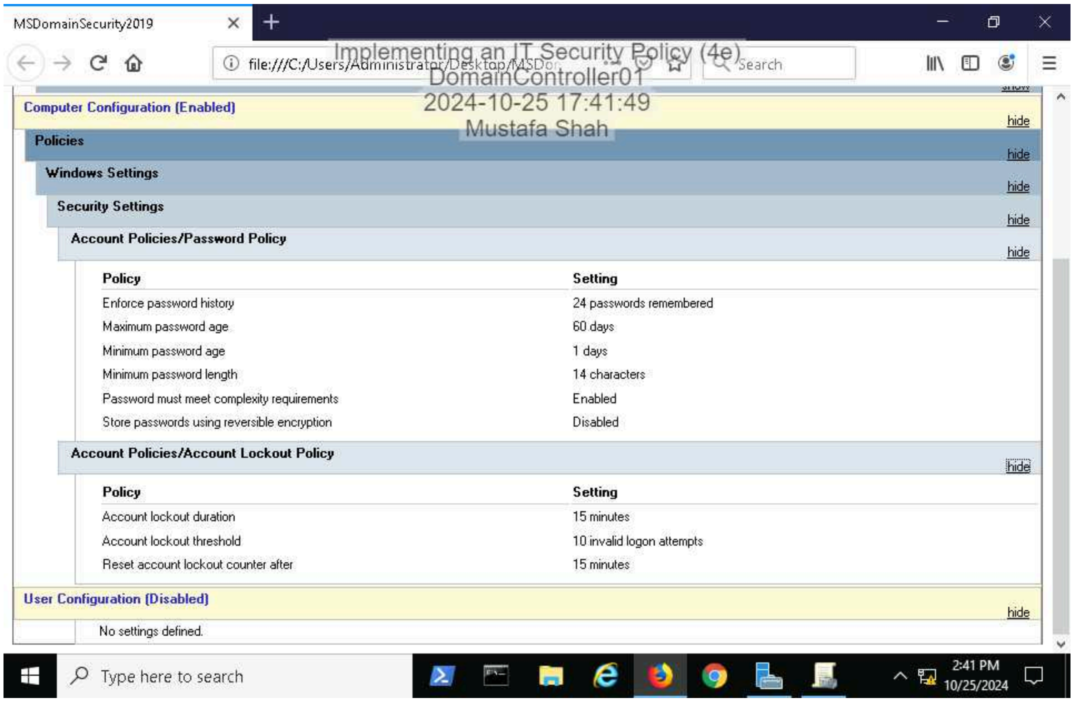
Status Details

DC01.securelabsondemand.com is the baseline domain controller for this domain. Change

No Infrastructure Status information exists for this domain.

Click the Detect Now button below to gather infrastructure status from all of the domain controllers in this domain.

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



MSDomainSecurity2019
file:///C:/Users/Administrator/Desktop/MSDo
Search
Implementing an IT Security Policy (4e)
DomainController01
2024-10-25 17:41:49
Mustafa Shah

Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Account Policies/Password Policy

Policy	Setting
Enforce password history	24 passwords remembered
Maximum password age	60 days
Minimum password age	1 days
Minimum password length	14 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Account Policies/Account Lockout Policy

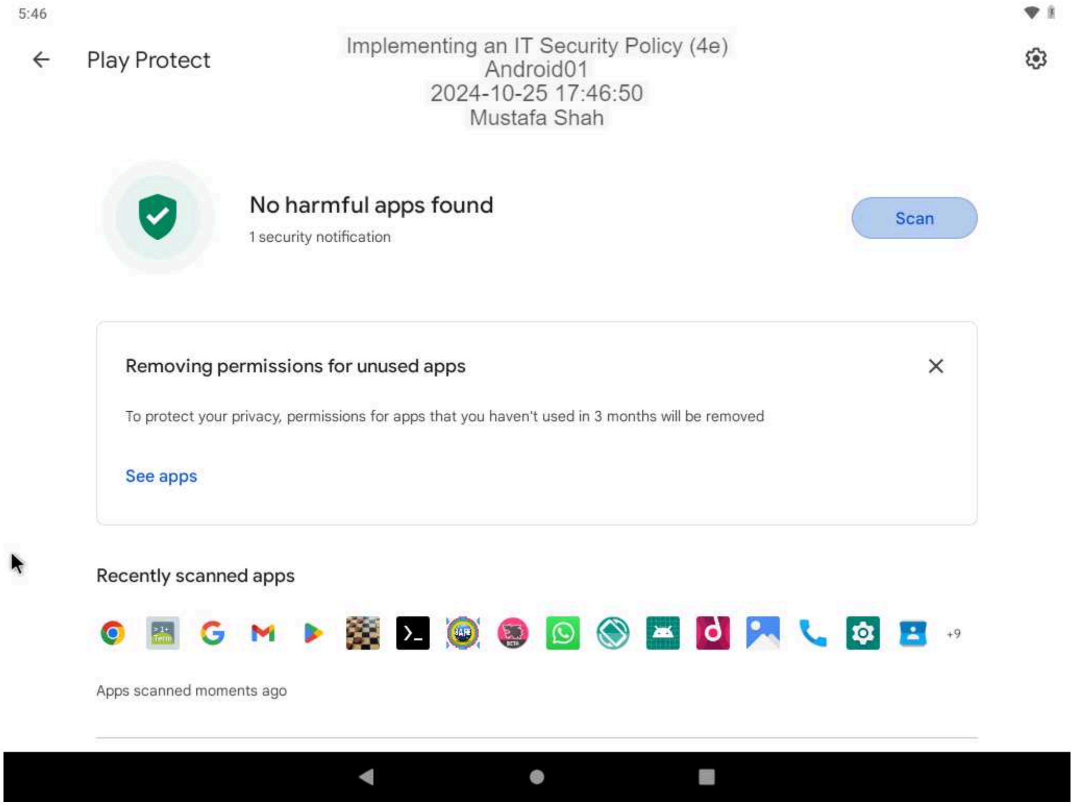
Policy	Setting
Account lockout duration	15 minutes
Account lockout threshold	10 invalid logon attempts
Reset account lockout counter after	15 minutes

User Configuration (Disabled)

No settings defined.

Part 2: Implement a Mobile Device Security Policy

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



Implementing an IT Security Policy (4e)
Android01
2024-10-25 17:46:50
Mustafa Shah

No harmful apps found

1 security notification

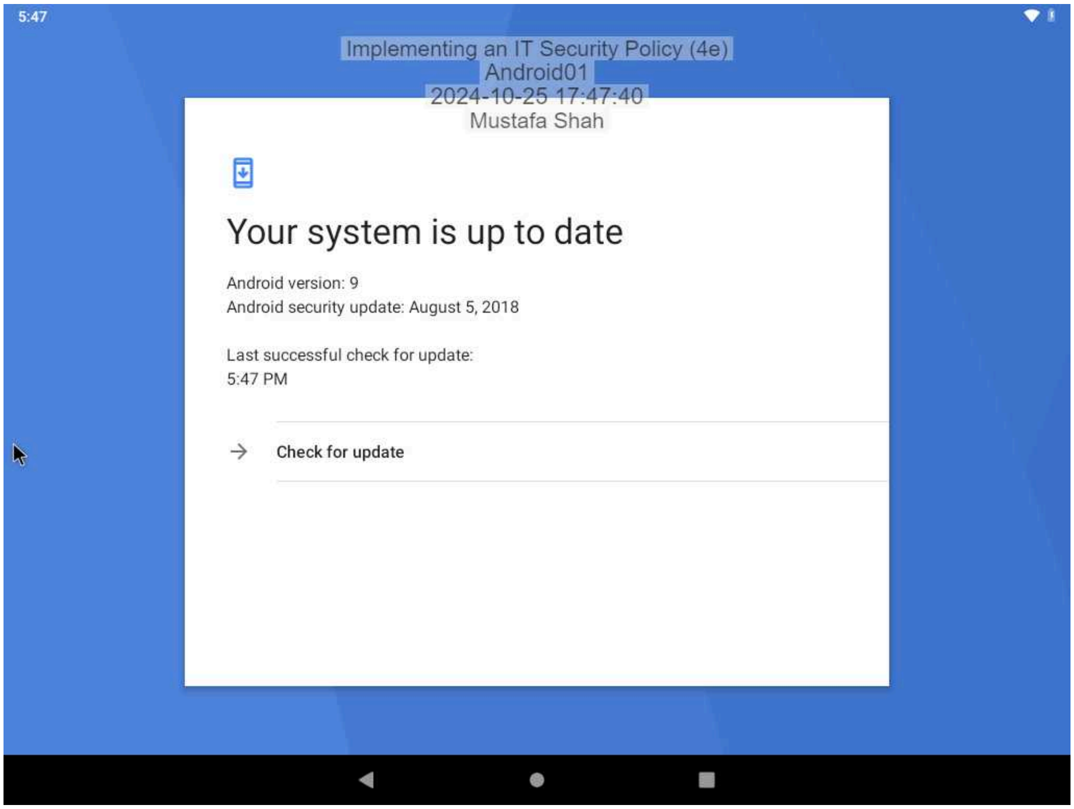
Removing permissions for unused apps

To protect your privacy, permissions for apps that you haven't used in 3 months will be removed

Recently scanned apps

Apps scanned moments ago

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



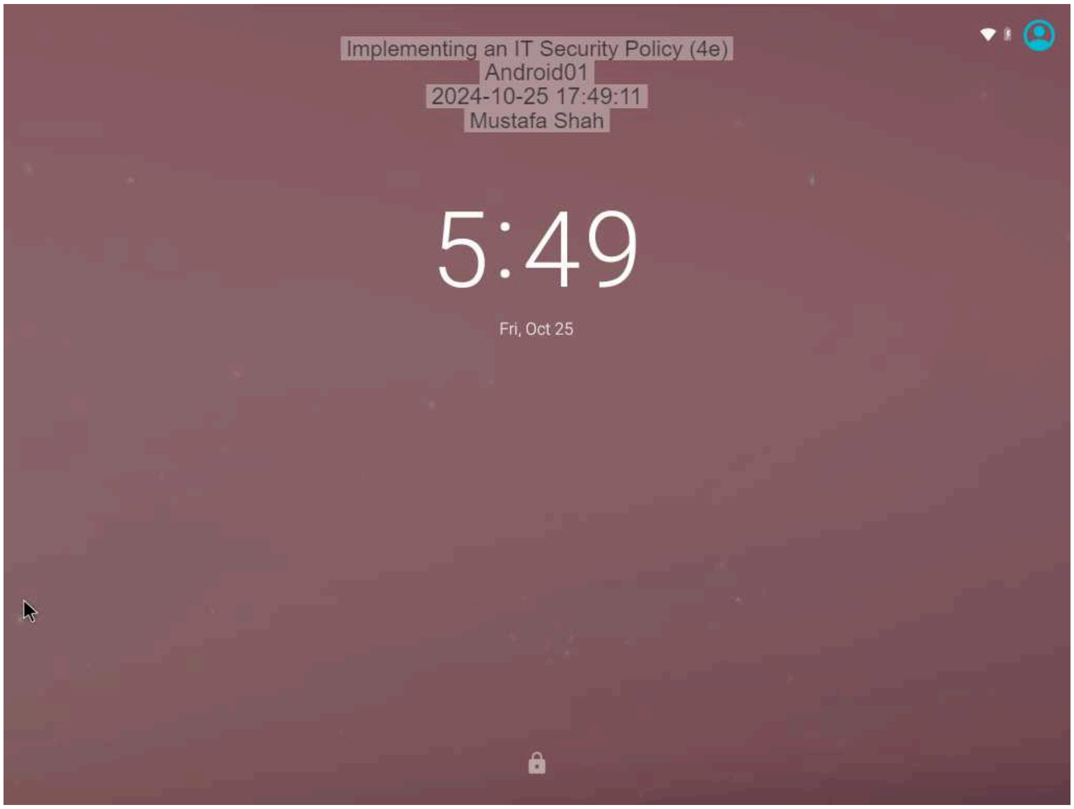
Implementing an IT Security Policy (4e)
Android01
2024-10-25 17:47:40
Mustafa Shah

Your system is up to date

Android version: 9
Android security update: August 5, 2018

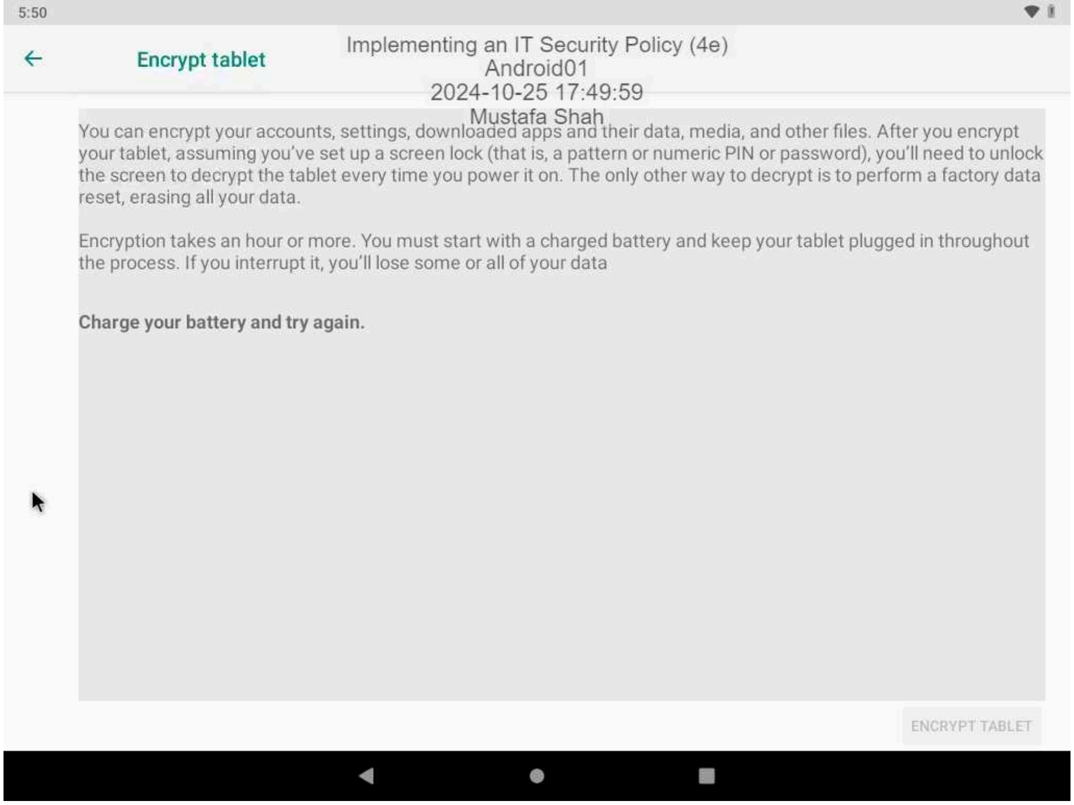
Last successful check for update:
5:47 PM

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



Implementing an IT Security Policy (4e)
Android01
2024-10-25 17:49:11
Mustafa Shah

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



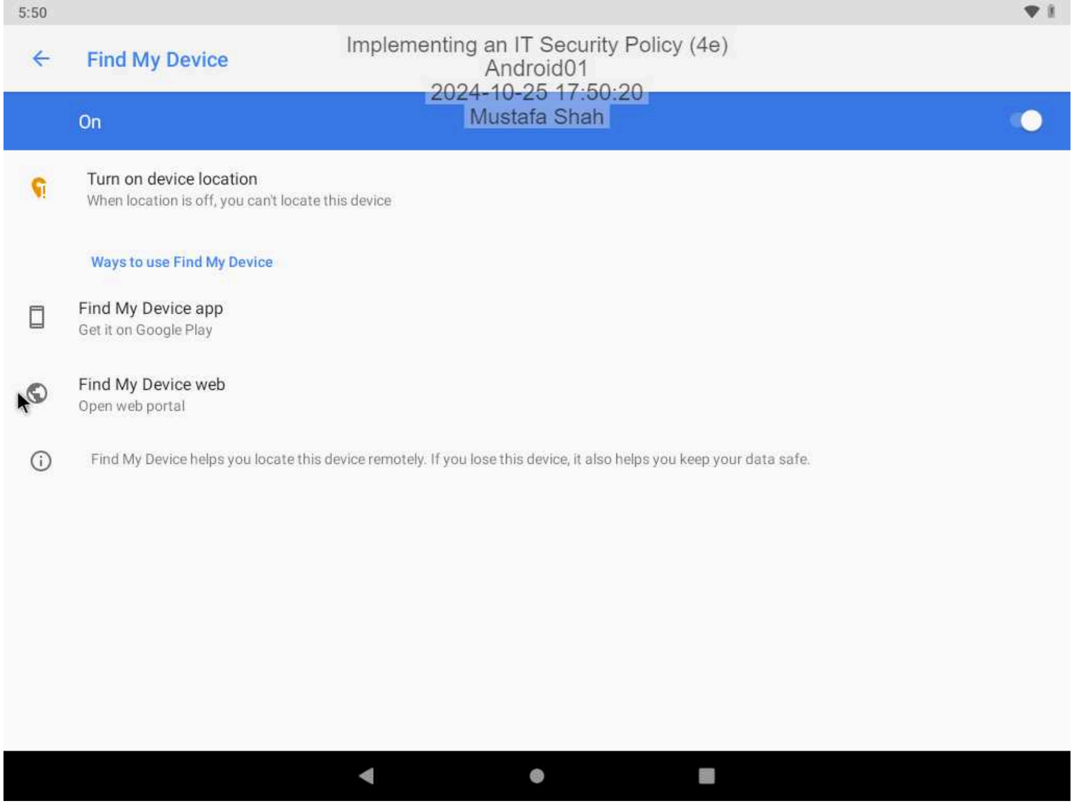
Implementing an IT Security Policy (4e)
Android01
2024-10-25 17:49:59
Mustafa Shah

You can encrypt your accounts, settings, downloaded apps and their data, media, and other files. After you encrypt your tablet, assuming you've set up a screen lock (that is, a pattern or numeric PIN or password), you'll need to unlock the screen to decrypt the tablet every time you power it on. The only other way to decrypt is to perform a factory data reset, erasing all your data.

Encryption takes an hour or more. You must start with a charged battery and keep your tablet plugged in throughout the process. If you interrupt it, you'll lose some or all of your data

Charge your battery and try again.

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



Implementing an IT Security Policy (4e)
Android01
2024-10-25 17:50:20
Mustafa Shah

On

Turn on device location
When location is off, you can't locate this device

Ways to use Find My Device

Find My Device app
Get it on Google Play

Find My Device web
Open web portal

Find My Device helps you locate this device remotely. If you lose this device, it also helps you keep your data safe.

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.

Prohibition of Illegal Activities: Most AUPs explicitly ban any use of IT resources for illegal purposes, such as accessing prohibited content, engaging in fraudulent activity, or downloading unauthorized software. This prevents legal repercussions for the organization and protects its reputation.
Restrictions on Personal Use: Many AUPs set boundaries on personal use of company resources, limiting activities like excessive personal browsing or social media use. This reduces distractions and improves productivity while also minimizing potential cybersecurity risks from non-work-related websites.
Confidentiality and Data Protection: AUPs often emphasize safeguarding sensitive data, prohibiting unauthorized sharing of proprietary information, and requiring adherence to data protection standards. This is crucial for compliance with regulations such as GDPR and HIPAA, helping protect customer and company data from breaches.
BYOD (Bring Your Own Device) Policies: With many employees using personal devices for work, AUPs commonly include rules for securing these devices, such as requiring encryption or VPN use. This minimizes the risk of security vulnerabilities that could be introduced through personal devices on the company network
Enforcement and Consequences: Clearly outlining consequences for violations is vital in AUPs to ensure users take them seriously. Typical consequences include warnings, revocation of access, or even legal action, depending on the severity of the breach. This not only reinforces policy compliance but also emphasizes the organization’s commitment to security and ethical standards.
Sources:https://www.business.com/articles/acceptable-use-policy/https://edtechmagazine.com/higher/article/2023/03/acceptable-use-policies-perfconhttps://resources.workable.com/acceptable-use-policy-template

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.

Data Collection Practices: Many policies detail the type of data collected and whether it’s provided by users directly or gathered automatically through cookies and tracking technologies. This disclosure allows users to understand the scope of data collection and choose to engage accordingly.
Data Usage Information: Policies also explain how collected data will be used, covering activities like personalization, marketing, and analytics. This transparency helps users understand why their data is necessary and builds trust in the company’s data handling practices.
Third-Party Data Sharing: Companies often clarify if and when data is shared with third parties, such as advertisers or analytics providers, including the protective measures in place to secure shared data. This is important for user privacy, as it reassures them that data sharing is controlled and secure
Data Protection Measures: Policies commonly outline data protection practices, such as encryption, access restrictions, and regular security audits. This demonstrates a company’s commitment to safeguarding user data against breaches and unauthorized access, helping build confidence in data privacy.
Data Retention and Deletion Policies: Informing users about data retention duration and deletion procedures ensures users know that their data won’t be kept indefinitely, thus aligning with data minimization principles found in regulations like GDPR.
Sources:https://www.privacypolicies.com/blog/privacy-policy-template/https://www.websitepolicies.com/blog/how-to-write-a-privacy-policyhttps://termly.io/resources/articles/why-you-need-a-privacy-policy/