ASSIGNMENT-2: System Hardening

-SPR 320

Name: Syed Mujahid Hamid Ali

Student ID: 161202213

Group Members:

1.	Khondoker Ishmum Muhammad	155895212
2.	Yannish Kumar Ballachandher Sreedevi	154915219

Table of Content

System and Environment Description

The system that I along with my partners have decided to harden for this assignment is Windows Server 2019. This is because Windows Server is more secure and this version especially comes with ATP, which is Advanced Threat Protection and it meant that threats were actively blocked instead of being blocked passively in the previous versions. Another advantage was that if in future we want to migrate to another operating system, this server will be highly compatible as it has many features which are like already existing operating systems. For example, if we look at the GUI of this server and Windows 10, we can see a lot of similarities.

The environment that we have decided to work on is in a small business. A small business is a privately owned company that has lesser employees and annual revenue than a regular sized business. By small, it means the definition given for different industries by the National administrations which look after the businesses in the country. An example would be that in Canada, if a company has less than 100 employees but more than 5 employees, it is considered as a small business.

The CIS controls that I thought would be best to use in this situation are:

1. Inventory and Control of Software Assets (Control 2)
2. Data Protection (Control 3)
3. Secure Configuration of Enterprise Assets and Software (Control 4)
4. Account Management (Control 5)
5. Continuous Vulnerability Management (Control 7)
6. Audit Log Management (Control 8)
7. Email and Web Browser Protections (Control 9)
8. Malware Defenses (Control 10)
9. Data Recovery (Control 11)
10. Application Software Security (Control 16)
11. Incident Response Management (Control 17)
12. Penetration Testing (Control 18)

Risk-Based Decisions

The risks that a small business would face could be majorly keeping weak passwords, improper configurations of firewalls due to lack of educated employees, bad auditing and documenting system and policies, etc.

Many small business owners do not really focus on these because they think that hackers and different attackers would target bigger firms. But they do not realize the amount of data that these companies hold which could be valuable and useful when it comes to attacking bigger organizations. This data could include customer information, bank details, user information, etc.

Implementation of Controls

The first policy that we have implemented is related to **Account Policies** and in it we have implemented the **Password Policies** given.

1. The first policy was to ensure that we set the "Enforce Password History" more than 24. But as we can see I have set it to 24 as well because that is the maximum limit. This is done so that users change passwords frequently which will make attackers harder to get credentials because the larger the number for this policy, the better as users will have to change passwords making it safer and more secure.

2. The next one is to change the "Maximum Password Age" to more than 0 and less than 365 days. This is done so that the password expires after the date that is mentioned. Over here I have kept this policy as 111 days. If it was kept 0 then it would mean that the password would never expire, which would also mean that if an attacker gets the password without the user knowing then there can be an intruder, which is very dangerous. Instead of reminding manually to change the passwords this is better as Windows itself will give a notification for changing the password.

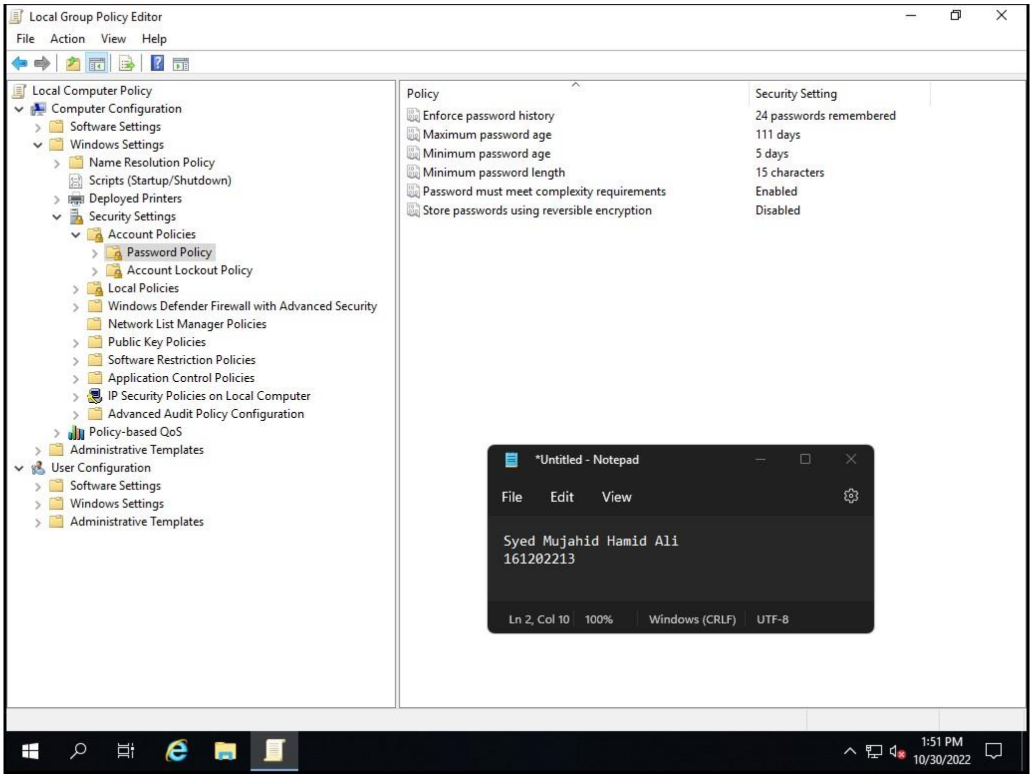
3. The next one is to change the "Minimum Password Age" to one or more days. Her I have chosen 5 because it is more than one, but it is not that long for keeping a password the same. This is done to ensure that users do not face a dilemma that their passwords are secure at any cost. An attacker will not directly attempt to get the password. They will get some prior knowledge and will narrow down the probabilities of having a password.

4. The next one is to ensure that the "Minimum Password Length" is set to 14 or more characters. I have set it to 15 because I think it is an ideal length for keeping a password; not too short nor too long. The reason we do this is because the longer the length, the harder it is for guessing the password because there will be way more permutations and combinations. Another good thing about this is that if there is a typing error made while trying to log in, the account can be reported if multiple attempts have been made.

5. The next one is to ensure that the "Password must meet complexity requirements" is set to enabled. This is done so that the passwords have a certain level of complexity which will make it harder for an attacker to guess. By complexity here, we mean that the password should include variety of levels like special characters, numbers, combination of uppercase and lowercase letters, etc.

6. **6.** The next one is to disable “Storing passwords using reversible encryption”. This is done because storing them in such a way would simply mean storing them in plaintext. This will strengthen our system as well because if this is enabled then the passwords are stored in a weaker format which will be more suspicious when being attacked and thus weakens the security of our system.

This is the screenshot that shows that I have configured the policies and ensured that they are best in terms of security.



Policy	Security Setting
Enforce password history	24 passwords remembered
Maximum password age	111 days
Minimum password age	5 days
Minimum password length	15 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

```
Syed Mujahid Hamid Ali
161202213
```

The next policy that we implemented are the **<u>Local Policies</u>** and we have applied the **<u>User Rights Assignment</u>**.

1. **1.** The first one is to ensure that “Adjust memory quotas for a process” is set to the groups Administrators, LOCAL SERVICE and NETWORK SERVICE. This is because this setting allows a user to adjust the amount of memory that is available to a process. This can be dangerous if assigned to wrong group of users because this right can be used to start a DoS (Denial of Service) attack which can be done by assigning the maximum memory size for a process the attacker wants, which will cause other important and critical applications to fail.

2. **2.** The next one is to ensure that “Create a token object” is set to no one. This is because this control gives the right to create tokens, which can be used in providing access to sensitive data. If this is given in wrong hands, attackers can

prioritize this account and then they will get access to creating token in which they will create as an administrator or a user who has the right to view sensitive data. This way it can be either used to cause a data breach or a DoS attack.

3. The next one is to ensure that “Deny log on as a batch job” is set to Guests. This is because the right allows to schedule jobs or create tasks which can use and consume majority of the system’s resources. This could be dangerous as it might cause a DoS condition.

4. The next one is to ensure that “Deny log on as a service” is set to Guests as well. This is because this right will determine which accounts are prevented from registering a process as a service. If assigned to the wrong group, some service might not be able to start and if these applications include critical ones, then the system could become a target for a DoS attack.

5. The next one is to ensure that “Force shutdown from a remote system” is set to only Administrators. This is because this right will allow authorized users to shut down computers from remote locations. If assigned to wrong group, they can shut down the system from their remote machine and then it will not be able to take any service requests, which can be used to cause a DoS condition to occur.

6. The next one is to ensure that “Increase scheduling priority” is set to Administrators and Windows Manager. This is because this right allows to determine if a user can change the priority class of a process. This can be dangerous if not assigned to the right groups because a user might increase the class for a process to real time which would decrease the time for other process which can include critical ones as well. Then this might cause a DoS condition as well.

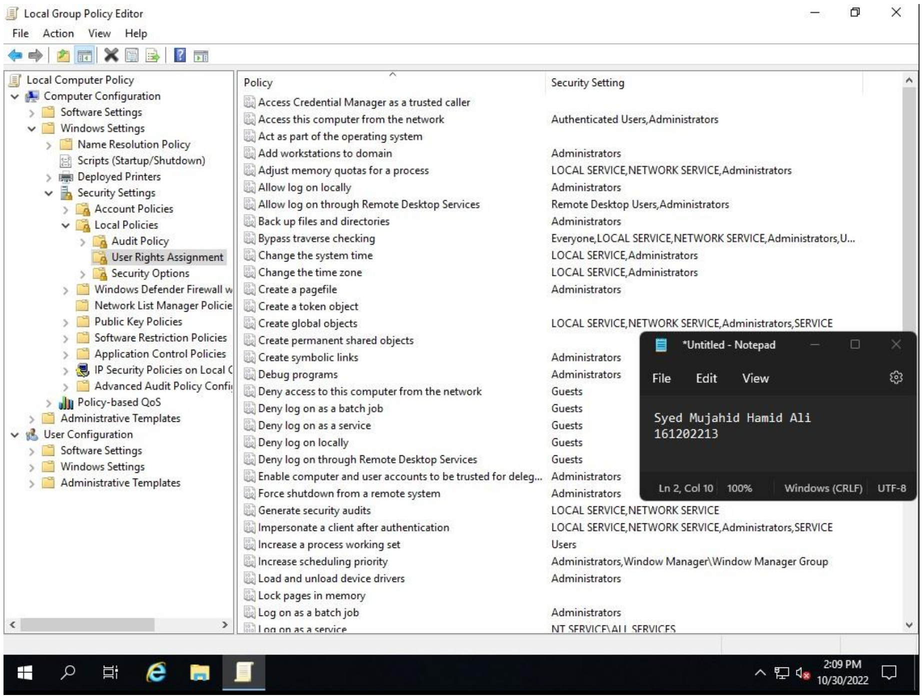
7. The next one is to ensure that “Lock pages in memory” is set to no one because this right allows processed to keep data in the physical memory and will prevent from paging the data into the virtual memory. If a user has access to this right, then they can assign physical memory to several processes which will leave very less memory for other process which could include critical ones and then it will result in a DoS condition.

8. The next one is to ensure that “Modify firmware environment values” is set to only Administrators because this policy allows users to change environment values that might affect hardware configuration. If these changes are made by some user who does not know, then it might cause hardware failure which could result in a DoS condition or data corruption.

9. The next one is to ensure that “Perform volume maintenance tasks” is set to only Administrators because this will allow users to manage the disk configuration. If given to wrong group of users, they can delete a volume of disk which could result in data loss as well as a DoS condition.

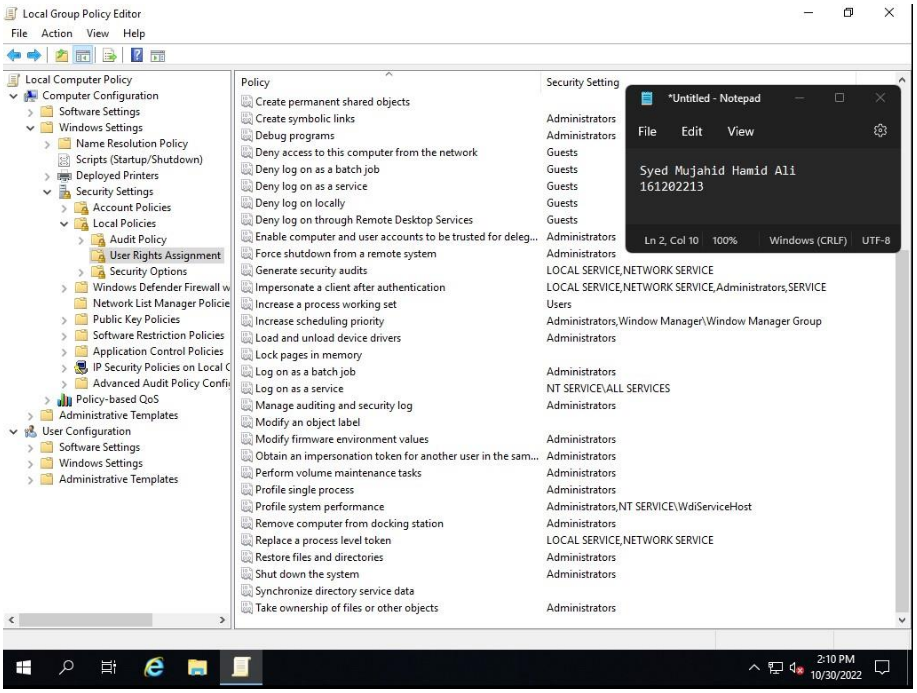
10. The next one is to ensure that “Take ownership of files or other objects” is set to only Administrators because this policy allows assigned users to take ownership of objects like files. This could be dangerous as it also allows to make changes in an object regardless of the permissions that are already set on it, which could result in data loss, data corruption and possibly a DoS condition.

These are the screenshots which show that I have implemented the above policies alongside some others as well which will protect me from different types of threats.



Policy	Security Setting
Access Credential Manager as a trusted caller	
Access this computer from the network	Authenticated Users,Administrators
Act as part of the operating system	
Add workstations to domain	Administrators
Adjust memory quotas for a process	LOCAL SERVICE,NETWORK SERVICE,Administrators
Allow log on locally	Administrators
Allow log on through Remote Desktop Services	Remote Desktop Users,Administrators
Back up files and directories	Administrators
Bypass traverse checking	Everyone,LOCAL SERVICE,NETWORK SERVICE,Administrators,U...
Change the system time	LOCAL SERVICE,Administrators
Change the time zone	LOCAL SERVICE,Administrators
Create a pagefile	Administrators
Create a token object	
Create global objects	LOCAL SERVICE,NETWORK SERVICE,Administrators,SERVICE
Create permanent shared objects	
Create symbolic links	Administrators
Debug programs	Administrators
Deny access to this computer from the network	Guests
Deny log on as a batch job	Guests
Deny log on as a service	Guests
Deny log on locally	Guests
Deny log on through Remote Desktop Services	Guests
Enable computer and user accounts to be trusted for deleg...	Administrators
Force shutdown from a remote system	Administrators
Generate security audits	LOCAL SERVICE,NETWORK SERVICE
Impersonate a client after authentication	LOCAL SERVICE,NETWORK SERVICE,Administrators,SERVICE
Increase a process working set	Users
Increase scheduling priority	Administrators,Window Manager\Window Manager Group
Load and unload device drivers	Administrators
Lock pages in memory	
Log on as a batch job	Administrators
Log on as a service	NT SERVICE\ALL SERVICES

```
Syed Mujahid Hamid Ali
161202213
```



Policy	Security Setting
Create permanent shared objects	
Create symbolic links	Administrators
Debug programs	Administrators
Deny access to this computer from the network	Guests
Deny log on as a batch job	Guests
Deny log on as a service	Guests
Deny log on locally	Guests
Deny log on through Remote Desktop Services	Guests
Enable computer and user accounts to be trusted for deleg...	Administrators
Force shutdown from a remote system	Administrators
Generate security audits	LOCAL SERVICE,NETWORK SERVICE
Impersonate a client after authentication	LOCAL SERVICE,NETWORK SERVICE,Administrators,SERVICE
Increase a process working set	Users
Increase scheduling priority	Administrators,Window Manager\Window Manager Group
Load and unload device drivers	Administrators
Lock pages in memory	
Log on as a batch job	Administrators
Log on as a service	NT SERVICE\ALL SERVICES
Manage auditing and security log	Administrators
Modify an object label	
Modify firmware environment values	Administrators
Obtain an impersonation token for another user in the sam...	Administrators
Perform volume maintenance tasks	Administrators
Profile single process	Administrators
Profile system performance	Administrators,NT SERVICE\WdiServiceHost
Remove computer from docking station	Administrators
Replace a process level token	LOCAL SERVICE,NETWORK SERVICE
Restore files and directories	Administrators
Shut down the system	Administrators
Synchronize directory service data	
Take ownership of files or other objects	Administrators

```
Syed Mujahid Hamid Ali
161202213
```

The next policies that I have implemented under the **Local Policy** are the **Security Options**.

1. The first one is to ensure that “Audit: Shut down system immediately if unable to log security audits” is set to disabled. This is because the policy allows to determine if the system can shut down if it is unable to document the security events in the form of a log file. This can be dangerous if it is enabled because in some circumstances, if it is unable to document, evidence or important troubleshooting data may be unavailable when the incident is reviewed. Also, attackers might generate large amounts of these logs which can also cause the computer to shut down if this policy is enabled which could result in a DoS attack.

2. The next one is to enable the “Domain member: Require strong (Windows 2000 or later) session key” policy. This is done so that only secure channels ca be established with the domain controllers that will be able to encrypt the data flowing with a strong key. If not done, then attackers could infiltrate the channeling process and could cause data loss or leaks. This could also cause eavesdropping, which is a form of hacking in which data is read or changed while being channeled.

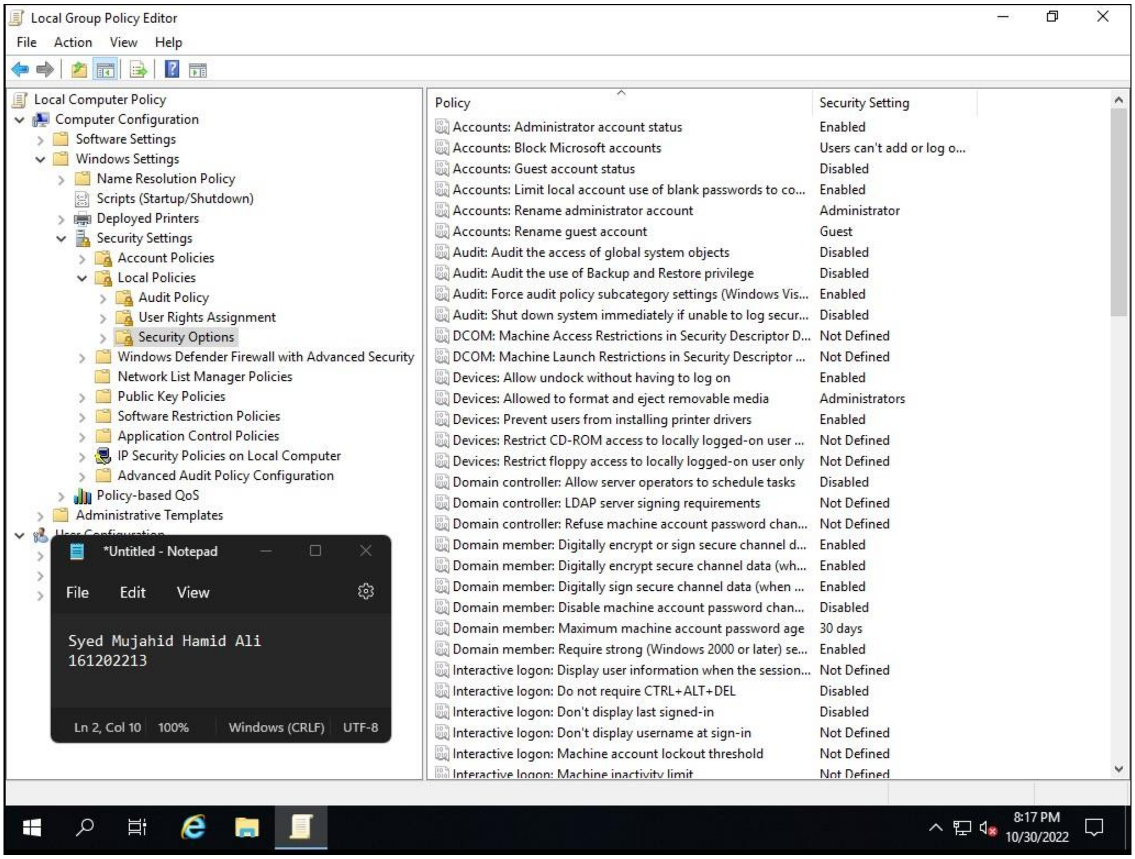
3. The next one is to ensure that “Network access: Let Everyone permissions apply to anonymous users” is set to disabled because this will allow us to determine the extra permissions given for unknown connections to the system. If enabled, an attacker could use an anonymous connection which will allow them to get hold of

data like account names and shared resources. This will be then used to either get passwords or launch attacks like DoS or social engineering attacks.

4. The next one is to disable the policy “Shutdown: Allow system to be shut down without having to log on” because this will determine if a system can be shut down when a user is not logged in. If it is enabled, then the shut down icon will be visible on the lock screen. This is dangerous because if someone else comes and either shuts down or restarts the system, the device can become a temporary cause for a DoS condition as the services will also stop in the middle of their processes.

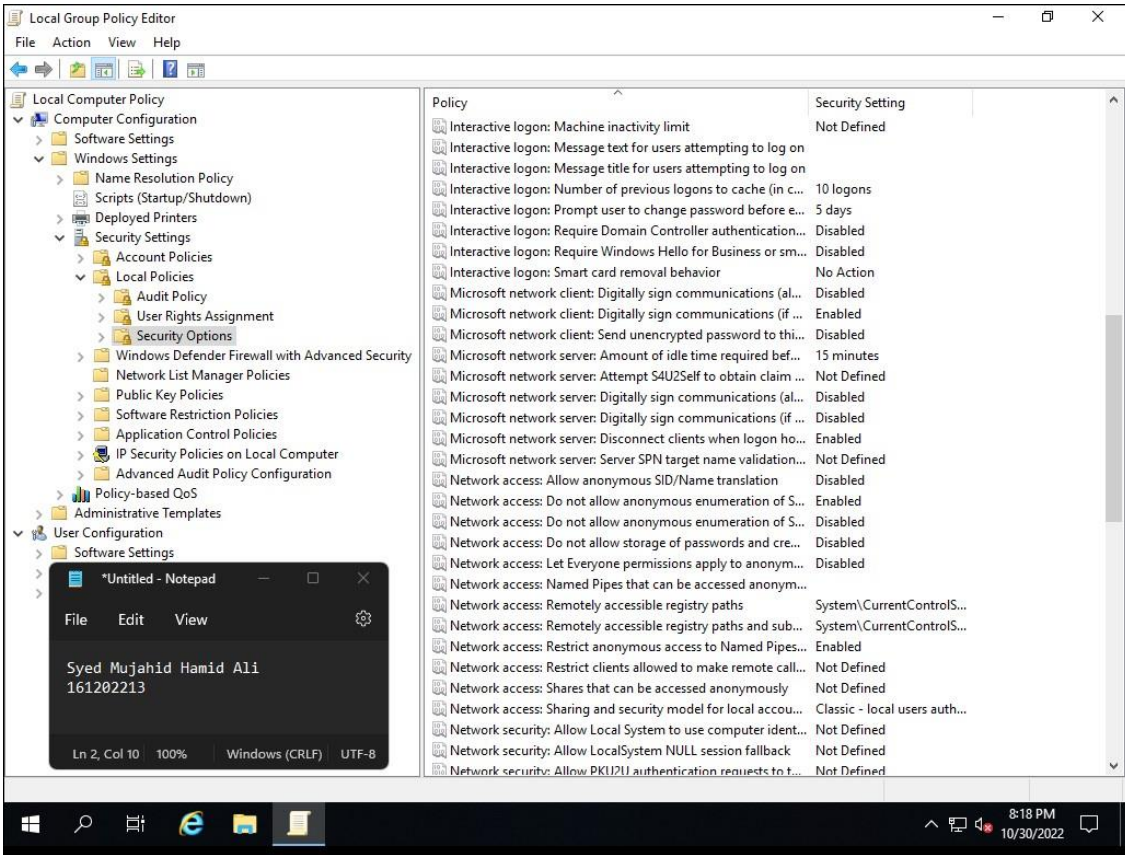
5. The next one is to enable the policy “System objects: Strengthen default permissions of internal system objects” because this will determine the strength of the whitelists for objects like registries or files. The default lists are itself stronger, so regular users cannot modify but read these. With this they will be able to infer who are the administrators, and if an attacker gets hands on these, he can cause data losses or possibly a data breach.

These screenshots show that I have made the correct changes to the above-mentioned policies.



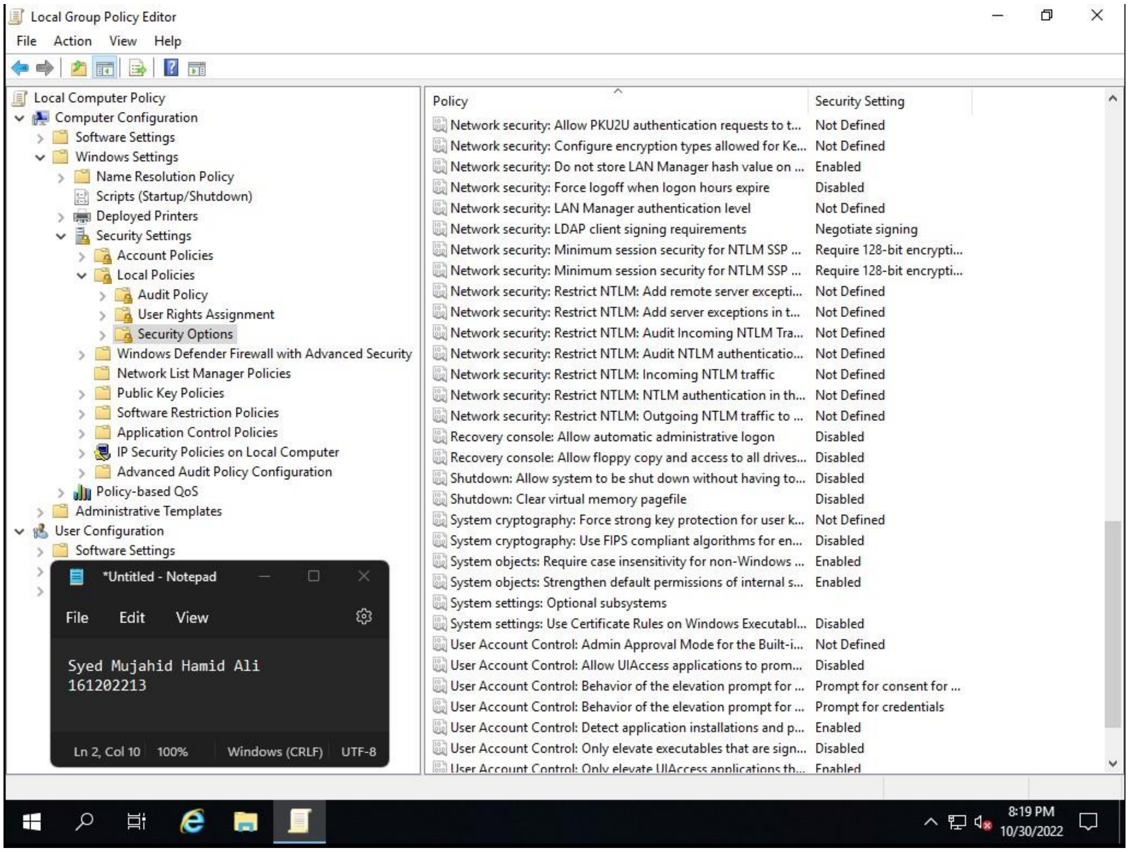
```
Syed Mujahid Hamid Ali
161202213
```

Policy	Security Setting
Accounts: Administrator account status	Enabled
Accounts: Block Microsoft accounts	Users can't add or log o...
Accounts: Guest account status	Disabled
Accounts: Limit local account use of blank passwords to co...	Enabled
Accounts: Rename administrator account	Administrator
Accounts: Rename guest account	Guest
Audit: Audit the access of global system objects	Disabled
Audit: Audit the use of Backup and Restore privilege	Disabled
Audit: Force audit policy subcategory settings (Windows Vis...	Enabled
Audit: Shut down system immediately if unable to log secur...	Disabled
DCOM: Machine Access Restrictions in Security Descriptor D...	Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor ...	Not Defined
Devices: Allow undock without having to log on	Enabled
Devices: Allowed to format and eject removable media	Administrators
Devices: Prevent users from installing printer drivers	Enabled
Devices: Restrict CD-ROM access to locally logged-on user ...	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Domain controller: Allow server operators to schedule tasks	Disabled
Domain controller: LDAP server signing requirements	Not Defined
Domain controller: Refuse machine account password chan...	Not Defined
Domain member: Digitally encrypt or sign secure channel d...	Enabled
Domain member: Digitally encrypt secure channel data (wh...	Enabled
Domain member: Digitally sign secure channel data (when ...	Enabled
Domain member: Disable machine account password chan...	Disabled
Domain member: Maximum machine account password age	30 days
Domain member: Require strong (Windows 2000 or later) se...	Enabled
Interactive logon: Display user information when the session...	Not Defined
Interactive logon: Do not require CTRL+ALT+DEL	Disabled
Interactive logon: Don't display last signed-in	Disabled
Interactive logon: Don't display username at sign-in	Not Defined
Interactive logon: Machine account lockout threshold	Not Defined
Interactive logon: Machine inactivity limit	Not Defined



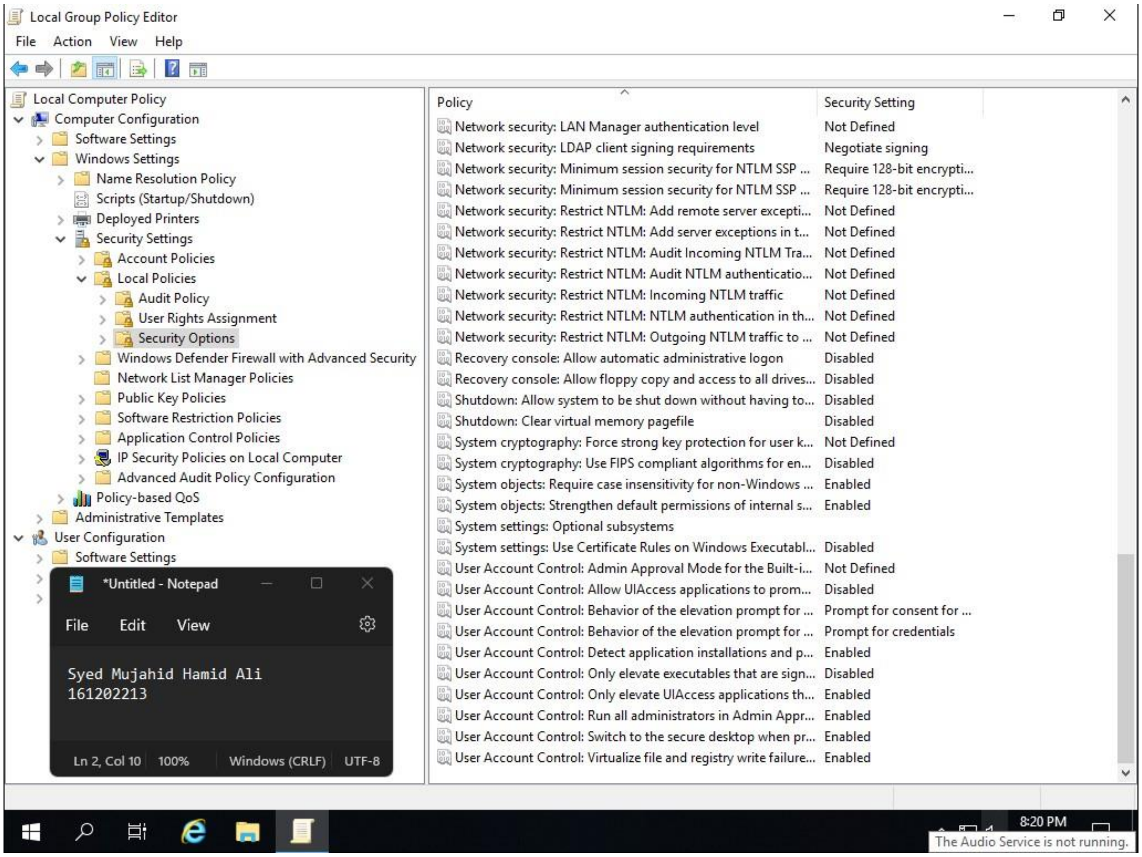
Syed Mujahid Hamid Ali
161202213

Policy	Security Setting
Interactive logon: Machine inactivity limit	Not Defined
Interactive logon: Message text for users attempting to log on	
Interactive logon: Message title for users attempting to log on	
Interactive logon: Number of previous logons to cache (in c...	10 logons
Interactive logon: Prompt user to change password before e...	5 days
Interactive logon: Require Domain Controller authentication...	Disabled
Interactive logon: Require Windows Hello for Business or sm...	Disabled
Interactive logon: Smart card removal behavior	No Action
Microsoft network client: Digitally sign communications (al...	Disabled
Microsoft network client: Digitally sign communications (if ...	Enabled
Microsoft network client: Send unencrypted password to thi...	Disabled
Microsoft network server: Amount of idle time required bef...	15 minutes
Microsoft network server: Attempt S4U2Self to obtain claim ...	Not Defined
Microsoft network server: Digitally sign communications (al...	Disabled
Microsoft network server: Digitally sign communications (if ...	Disabled
Microsoft network server: Disconnect clients when logon ho...	Enabled
Microsoft network server: Server SPN target name validation...	Not Defined
Network access: Allow anonymous SID/Name translation	Disabled
Network access: Do not allow anonymous enumeration of S...	Enabled
Network access: Do not allow anonymous enumeration of S...	Disabled
Network access: Do not allow storage of passwords and cre...	Disabled
Network access: Let Everyone permissions apply to anonym...	Disabled
Network access: Named Pipes that can be accessed anonym...	
Network access: Remotely accessible registry paths	System\CurrentControlS...
Network access: Remotely accessible registry paths and sub...	System\CurrentControlS...
Network access: Restrict anonymous access to Named Pipes...	Enabled
Network access: Restrict clients allowed to make remote call...	Not Defined
Network access: Shares that can be accessed anonymously	Not Defined
Network access: Sharing and security model for local accou...	Classic - local users auth...
Network security: Allow Local System to use computer ident...	Not Defined
Network security: Allow LocalSystem NULL session fallback	Not Defined
Network security: Allow PKU2U authentication requests to t...	Not Defined



Syed Mujahid Hamid Ali
161202213

Policy	Security Setting
Network security: Allow PKU2U authentication requests to t...	Not Defined
Network security: Configure encryption types allowed for Ke...	Not Defined
Network security: Do not store LAN Manager hash value on ...	Enabled
Network security: Force logoff when logon hours expire	Disabled
Network security: LAN Manager authentication level	Not Defined
Network security: LDAP client signing requirements	Negotiate signing
Network security: Minimum session security for NTLM SSP ...	Require 128-bit encrypti...
Network security: Minimum session security for NTLM SSP ...	Require 128-bit encrypti...
Network security: Restrict NTLM: Add remote server excepti...	Not Defined
Network security: Restrict NTLM: Add server exceptions in t...	Not Defined
Network security: Restrict NTLM: Audit Incoming NTLM Tra...	Not Defined
Network security: Restrict NTLM: Audit NTLM authenticatio...	Not Defined
Network security: Restrict NTLM: Incoming NTLM traffic	Not Defined
Network security: Restrict NTLM: NTLM authentication in th...	Not Defined
Network security: Restrict NTLM: Outgoing NTLM traffic to ...	Not Defined
Recovery console: Allow automatic administrative logon	Disabled
Recovery console: Allow floppy copy and access to all drives...	Disabled
Shutdown: Allow system to be shut down without having to...	Disabled
Shutdown: Clear virtual memory pagefile	Disabled
System cryptography: Force strong key protection for user k...	Not Defined
System cryptography: Use FIPS compliant algorithms for en...	Disabled
System objects: Require case insensitivity for non-Windows ...	Enabled
System objects: Strengthen default permissions of internal s...	Enabled
System settings: Optional subsystems	
System settings: Use Certificate Rules on Windows Executabl...	Disabled
User Account Control: Admin Approval Mode for the Built-i...	Not Defined
User Account Control: Allow UIAccess applications to prom...	Disabled
User Account Control: Behavior of the elevation prompt for ...	Prompt for consent for ...
User Account Control: Behavior of the elevation prompt for ...	Prompt for credentials
User Account Control: Detect application installations and p...	Enabled
User Account Control: Only elevate executables that are sign...	Disabled
User Account Control: Only elevate UIAccess applications th...	Enabled

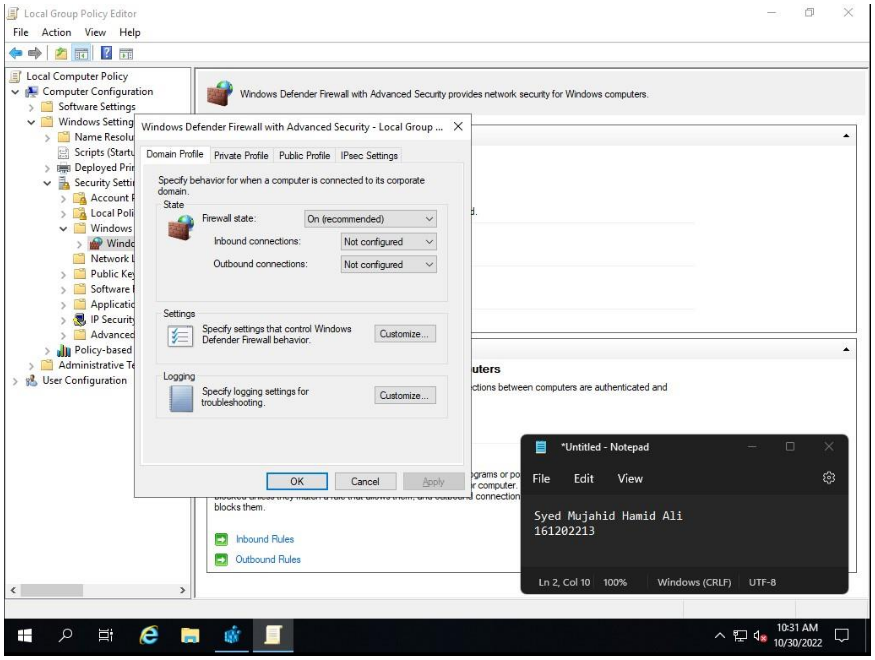


Policy	Security Setting
Network security: LAN Manager authentication level	Not Defined
Network security: LDAP client signing requirements	Negotiate signing
Network security: Minimum session security for NTLM SSP ...	Require 128-bit encrypti...
Network security: Minimum session security for NTLM SSP ...	Require 128-bit encrypti...
Network security: Restrict NTLM: Add remote server excepti...	Not Defined
Network security: Restrict NTLM: Add server exceptions in t...	Not Defined
Network security: Restrict NTLM: Audit Incoming NTLM Tra...	Not Defined
Network security: Restrict NTLM: Audit NTLM authenticatio...	Not Defined
Network security: Restrict NTLM: Incoming NTLM traffic	Not Defined
Network security: Restrict NTLM: NTLM authentication in th...	Not Defined
Network security: Restrict NTLM: Outgoing NTLM traffic to ...	Not Defined
Recovery console: Allow automatic administrative logon	Disabled
Recovery console: Allow floppy copy and access to all drives...	Disabled
Shutdown: Allow system to be shut down without having to...	Disabled
Shutdown: Clear virtual memory pagefile	Disabled
System cryptography: Force strong key protection for user k...	Not Defined
System cryptography: Use FIPS compliant algorithms for en...	Disabled
System objects: Require case insensitivity for non-Windows ...	Enabled
System objects: Strengthen default permissions of internal s...	Enabled
System settings: Optional subsystems	
System settings: Use Certificate Rules on Windows Executabl...	Disabled
User Account Control: Admin Approval Mode for the Built-i...	Not Defined
User Account Control: Allow UIAccess applications to prom...	Disabled
User Account Control: Behavior of the elevation prompt for ...	Prompt for consent for ...
User Account Control: Behavior of the elevation prompt for ...	Prompt for credentials
User Account Control: Detect application installations and p...	Enabled
User Account Control: Only elevate executables that are sign...	Disabled
User Account Control: Only elevate UIAccess applications th...	Enabled
User Account Control: Run all administrators in Admin Appr...	Enabled
User Account Control: Switch to the secure desktop when pr...	Enabled
User Account Control: Virtualize file and registry write failure...	Enabled

```
Syed Mujahid Hamid Ali
161202213
```

The next set of policies are for **Windows Defender Firewall with Advanced Security** and the first policy is to follow the recommendations given for the **Domain Profile**.

1. The first one is to ensure that the firewall start is set to On. This is done because if the state is turned off, none of the rules will be applied and all the traffic will be able to access the system, which will make it easier for an attacker to remotely exploit different vulnerabilities in the network service.



Windows Defender Firewall with Advanced Security - Local Group ...

Domain Profile | Private Profile | Public Profile | IPsec Settings

Specify behavior for when a computer is connected to its corporate domain.

State

Firewall state: On (recommended)

Inbound connections: Not configured

Outbound connections: Not configured

Settings

Specify settings that control Windows Defender Firewall behavior. Customize...

Logging

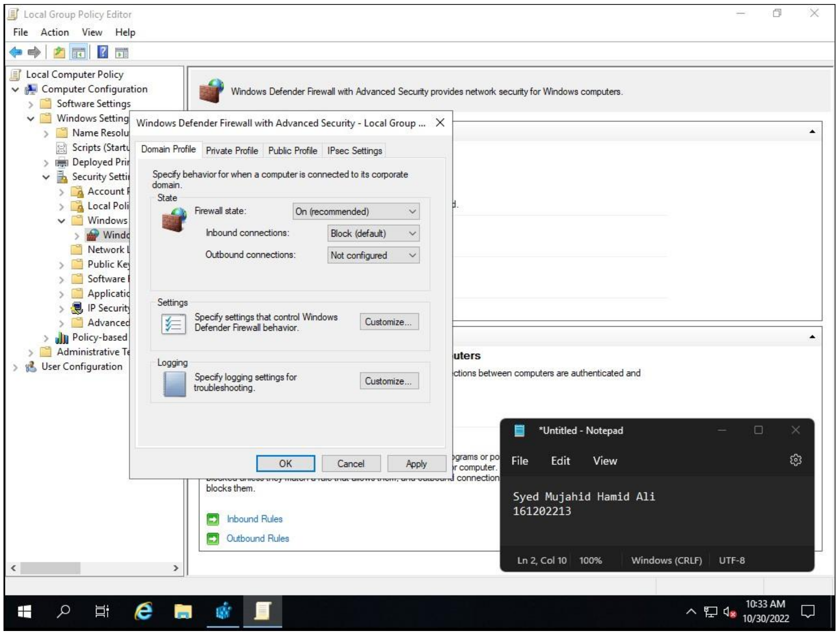
Specify logging settings for troubleshooting. Customize...

*Untitled - Notepad

```
Syed Mujahid Hamid Ali
161202213
```

10:31 AM 10/30/2022

2. The net one is to block all the inbound connections. This is done so that the connections that do not match the inbound firewall rules will be blocked. Else, it will be very easy for an attacker to exploit weaknesses if the firewall allows all traffic.



Windows Defender Firewall with Advanced Security - Local Group ...

Domain Profile | Private Profile | Public Profile | IPsec Settings

Specify behavior for when a computer is connected to its corporate domain.

State

Firewall state: On (recommended)

Inbound connections: Block (default)

Outbound connections: Not configured

Settings

Specify settings that control Windows Defender Firewall behavior. Customize...

Logging

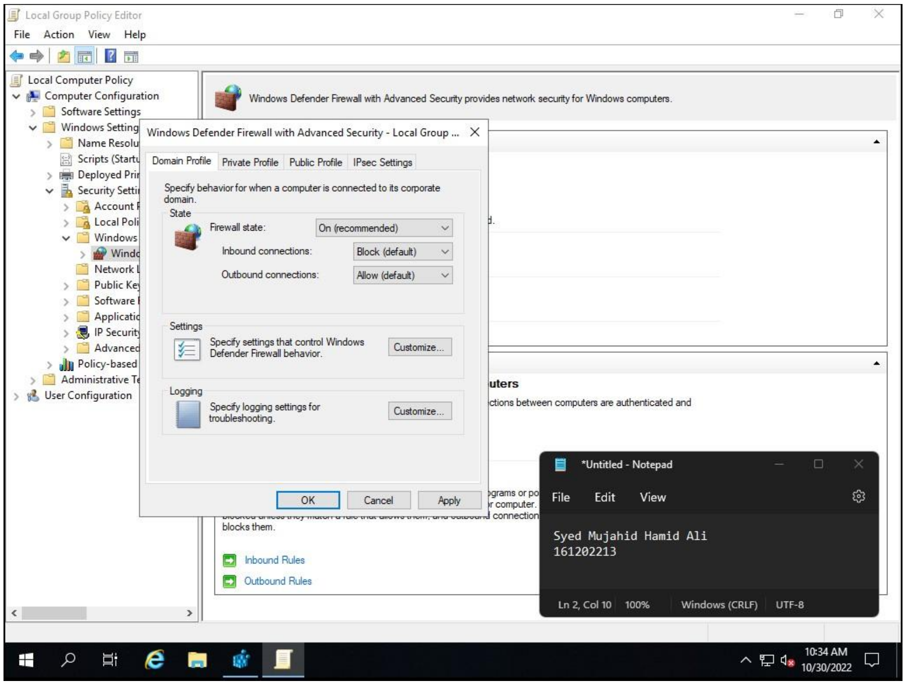
Specify logging settings for troubleshooting. Customize...

*Untitled - Notepad

```
Syed Mujahid Hamid Ali
161202213
```

10:33 AM 10/30/2022

3. The next one is to ensure that allow outbound connections are allowed. This is set as Allow because Microsoft itself recommends it and will allow all the connections except the ones that have a firewall rule that is explicitly blocking it.



Windows Defender Firewall with Advanced Security provides network security for Windows computers.

Windows Defender Firewall with Advanced Security - Local Group ...

Domain Profile | Private Profile | Public Profile | IPsec Settings

Specify behavior for when a computer is connected to its corporate domain.

State
Firewall state: On (recommended)
Inbound connections: Block (default)
Outbound connections: Allow (default)

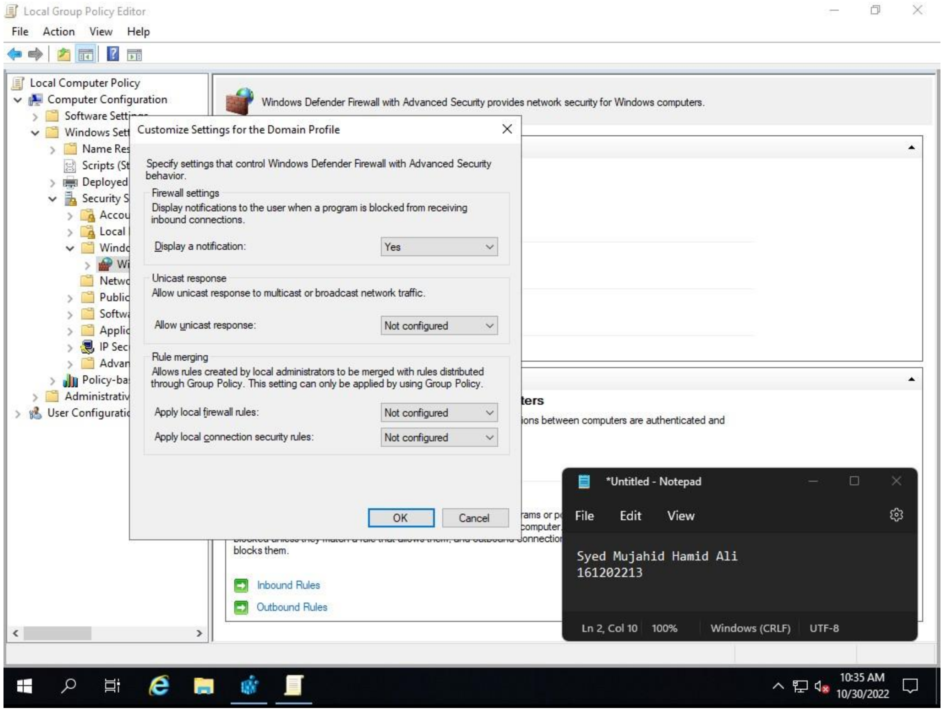
Settings
Specify settings that control Windows Defender Firewall behavior. Customize...

Logging
Specify logging settings for troubleshooting. Customize...

OK Cancel Apply

Syed Mujahid Hamid Ali
161202213

4. Next is to ensure that displaying a notification is set to No because if kept as Yes, users will continuously receive messages whenever an inbound connection is made. For this, whatever the user responds, it will be ignored as we have set all inbound connections to be blocked.



Windows Defender Firewall with Advanced Security provides network security for Windows computers.

Customize Settings for the Domain Profile

Specify settings that control Windows Defender Firewall with Advanced Security behavior.

Firewall settings
Display notifications to the user when a program is blocked from receiving inbound connections.
Display a notification: Yes

Unicast response
Allow unicast response to multicast or broadcast network traffic.
Allow unicast response: Not configured

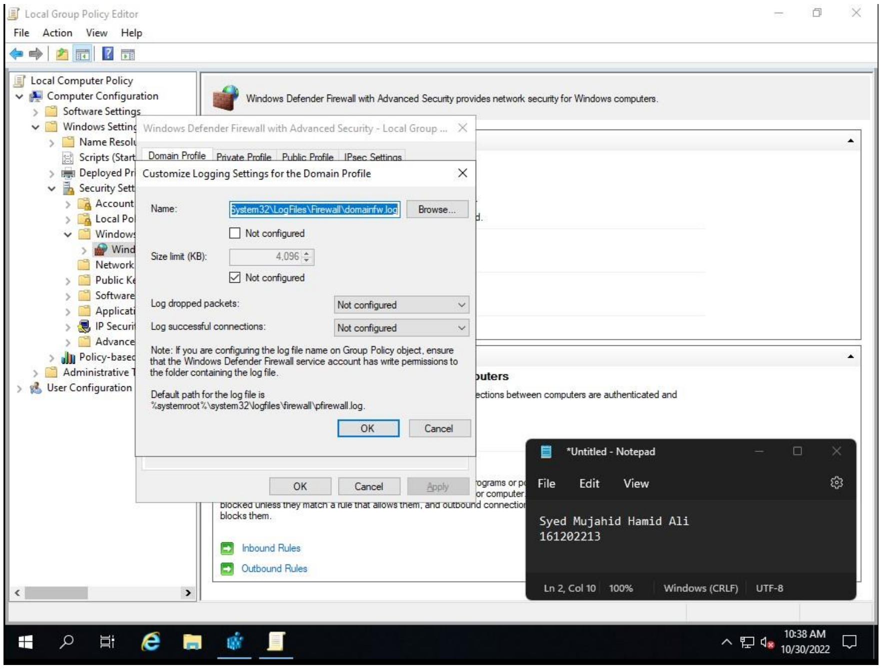
Rule merging
Allows rules created by local administrators to be merged with rules distributed through Group Policy. This setting can only be applied by using Group Policy.
Apply local firewall rules: Not configured
Apply local connection security rules: Not configured

OK Cancel

Syed Mujahid Hamid Ali
161202213

5. The next one is to set the log file in which Windows Firewall will store and document the events being made. This is done because if events are not recorded,

it becomes very difficult to determine the actual cause of suspicious activities done by malicious users or any other system problems that took place.



Customize Logging Settings for the Domain Profile

Name: System32\LogFiles\Firewall\domainfw.log

☐ Not configured

Size limit (KB): 4,096

☑ Not configured

Log dropped packets: Not configured

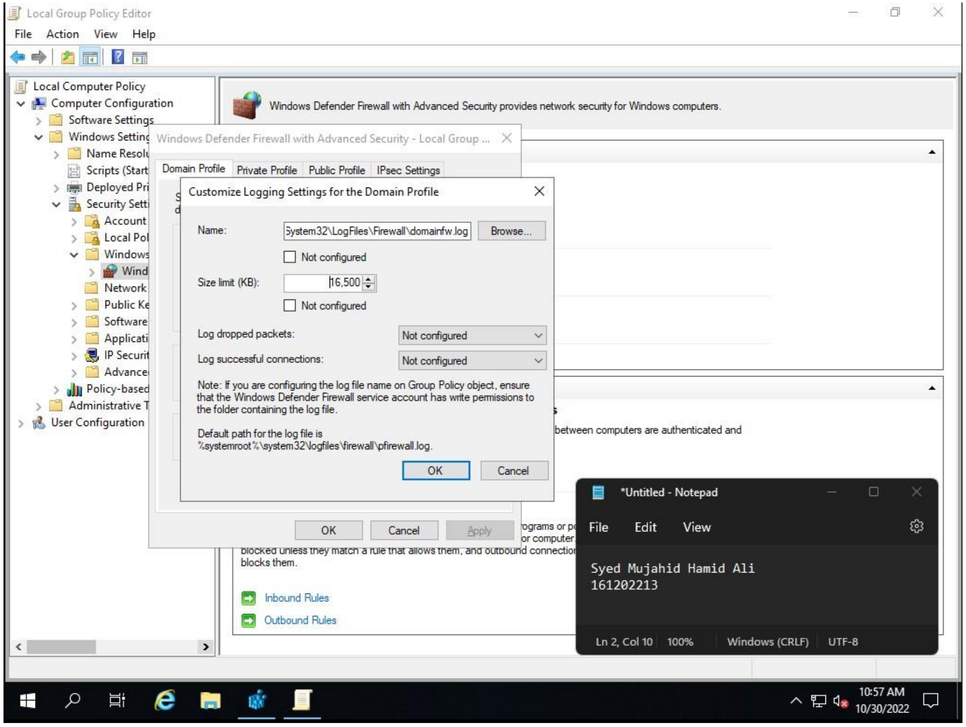
Log successful connections: Not configured

Note: If you are configuring the log file name on Group Policy object, ensure that the Windows Defender Firewall service account has write permissions to the folder containing the log file.

Default path for the log file is %systemroot%\system32\logfiles\firewall\pfirewall.log.

Syed Mujahid Hamid Ali
161202213

6. The next is to set the size limit to more than 16,384 KB. This is the file size allocation given to the log file being made to write and document all the events and once the file becomes full, old events will be overwritten by new ones.



Customize Logging Settings for the Domain Profile

Name: System32\LogFiles\Firewall\domainfw.log

☐ Not configured

Size limit (KB): 16,500

☐ Not configured

Log dropped packets: Not configured

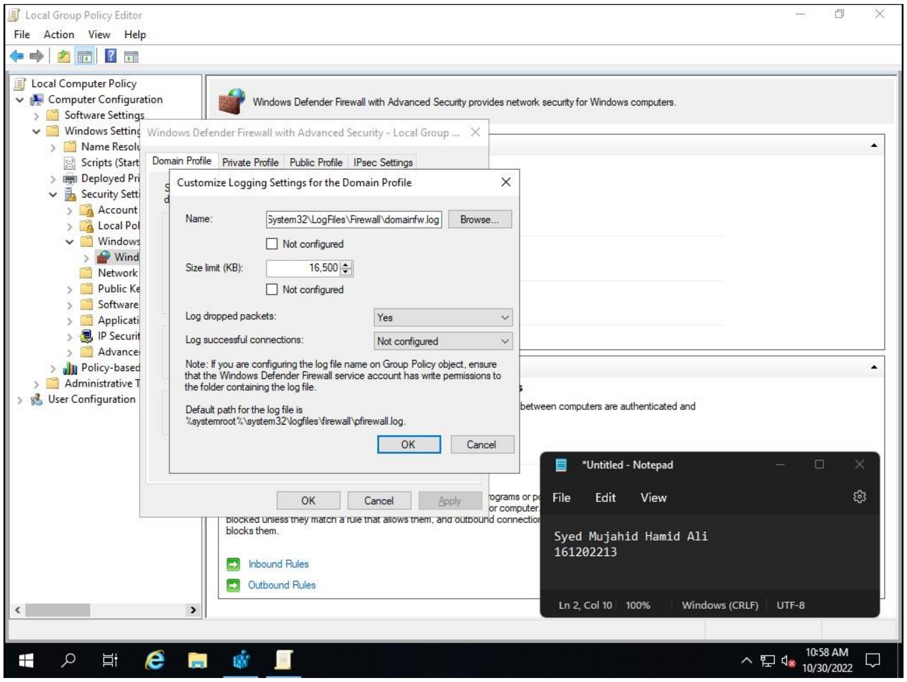
Log successful connections: Not configured

Note: If you are configuring the log file name on Group Policy object, ensure that the Windows Defender Firewall service account has write permissions to the folder containing the log file.

Default path for the log file is %systemroot%\system32\logfiles\firewall\pfirewall.log.

Syed Mujahid Hamid Ali
161202213

7. The next one is set log dropped packets as Yes because this will document all the packets that have been discarded when an inbound connection is attempted. This will also why and when the packet was dropped.



Local Group Policy Editor

Windows Defender Firewall with Advanced Security provides network security for Windows computers.

Windows Defender Firewall with Advanced Security - Local Group ...

Customize Logging Settings for the Domain Profile

Name: System32\LogFiles\Firewall\domainfw.log Browse...

□ Not configured

Size limit (KB): 16,500

□ Not configured

Log dropped packets: Yes

Log successful connections: Not configured

Note: If you are configuring the log file name on Group Policy object, ensure that the Windows Defender Firewall service account has write permissions to the folder containing the log file.

Default path for the log file is %systemroot%\system32\logfiles\firewall\pfirewall.log.

OK Cancel

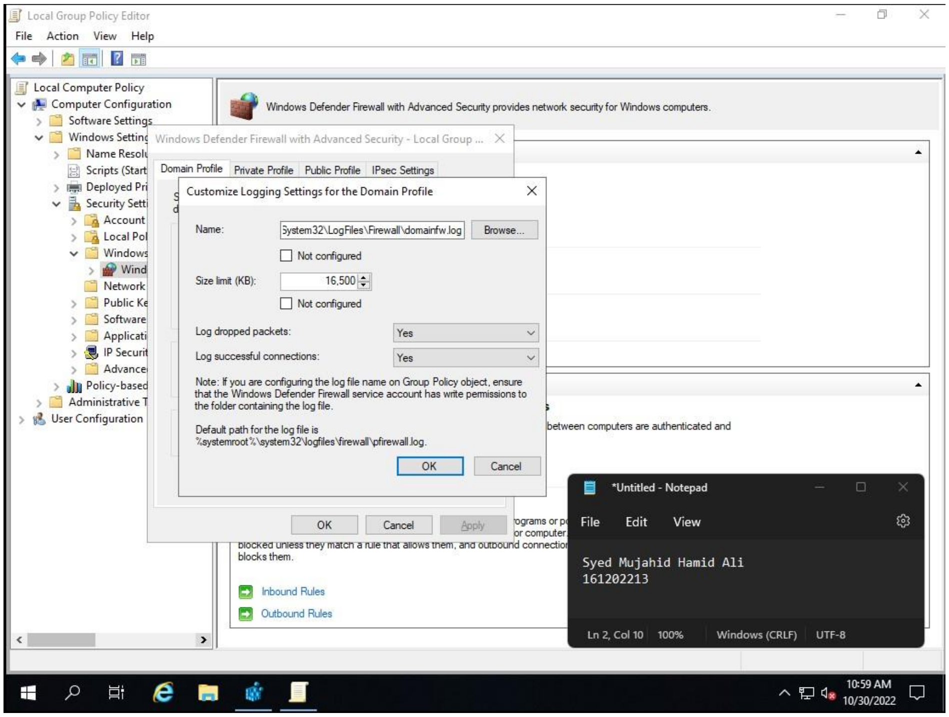
*Untitled - Notepad

Syed Mujahid Hamid Ali
161202213

Ln 2, Col 10 100% Windows (CRLF) UTF-8

10:58 AM 10/30/2022

8. The next one is to ensure that log successful connections are set to Yes as well because this does the opposite of the above policy. This will document the successful inbound connections being made. This will also record the when and why the connection was formed.



Local Group Policy Editor

Windows Defender Firewall with Advanced Security provides network security for Windows computers.

Windows Defender Firewall with Advanced Security - Local Group ...

Customize Logging Settings for the Domain Profile

Name: System32\LogFiles\Firewall\domainfw.log Browse...

□ Not configured

Size limit (KB): 16,500

□ Not configured

Log dropped packets: Yes

Log successful connections: Yes

Note: If you are configuring the log file name on Group Policy object, ensure that the Windows Defender Firewall service account has write permissions to the folder containing the log file.

Default path for the log file is %systemroot%\system32\logfiles\firewall\pfirewall.log.

OK Cancel

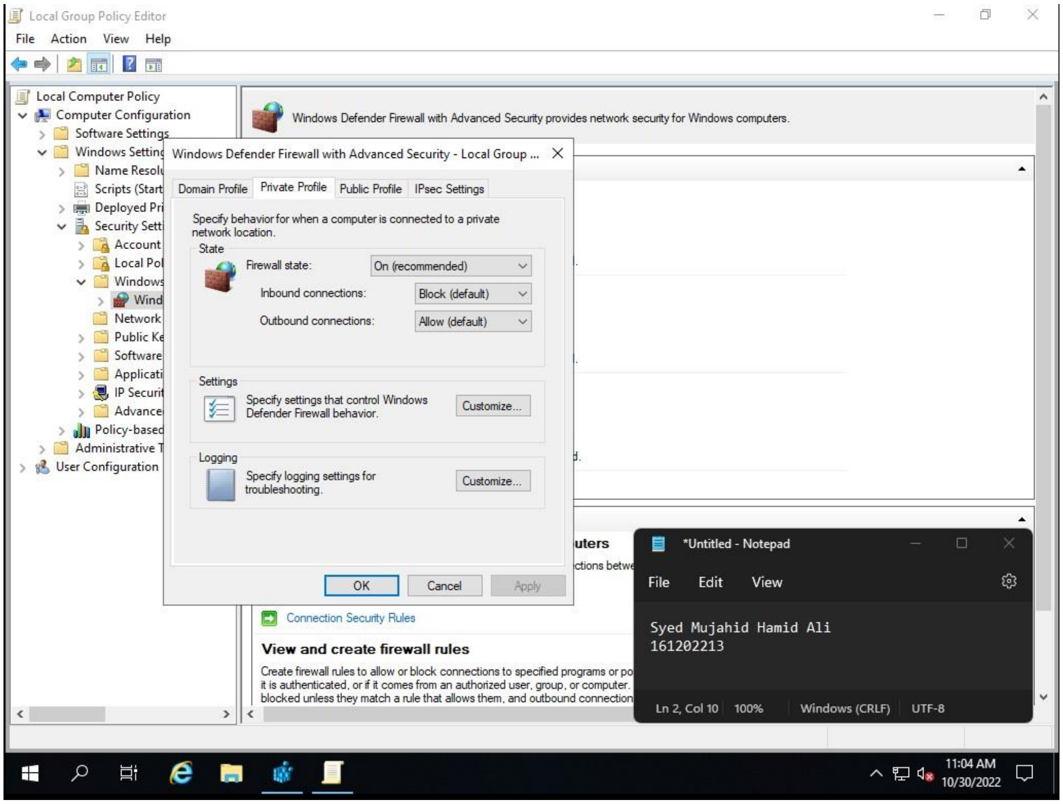
*Untitled - Notepad

Syed Mujahid Hamid Ali
161202213

Ln 2, Col 10 100% Windows (CRLF) UTF-8

10:59 AM 10/30/2022

The next one is to set the **Private Firewall**. This has the almost same policies as the above ones mentioned for the domain profile.



Windows Defender Firewall with Advanced Security provides network security for Windows computers.

Windows Defender Firewall with Advanced Security - Local Group ...

Domain Profile | Private Profile | Public Profile | IPsec Settings

Specify behavior for when a computer is connected to a private network location.

State

Firewall state: On (recommended)

Inbound connections: Block (default)

Outbound connections: Allow (default)

Settings

Specify settings that control Windows Defender Firewall behavior. Customize...

Logging

Specify logging settings for troubleshooting. Customize...

OK Cancel Apply

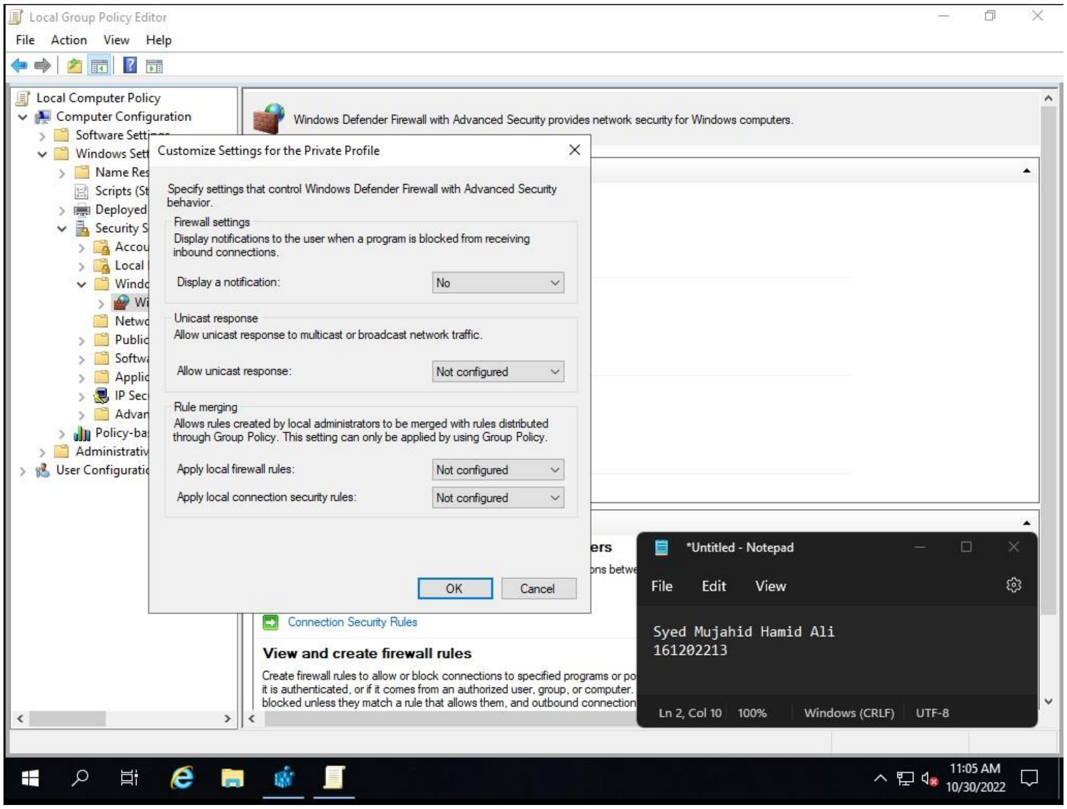
View and create firewall rules

Create firewall rules to allow or block connections to specified programs or po... it is authenticated, or if it comes from an authorized user, group, or computer. ... blocked unless they match a rule that allows them, and outbound connection...

*Untitled - Notepad

```
Syed Mujahid Hamid Ali
161202213
```

Ln 2, Col 10 100% Windows (CRLF) UTF-8



Windows Defender Firewall with Advanced Security provides network security for Windows computers.

Customize Settings for the Private Profile

Specify settings that control Windows Defender Firewall with Advanced Security behavior.

Firewall settings

Display notifications to the user when a program is blocked from receiving inbound connections.

Display a notification: No

Unicast response

Allow unicast response to multicast or broadcast network traffic.

Allow unicast response: Not configured

Rule merging

Allows rules created by local administrators to be merged with rules distributed through Group Policy. This setting can only be applied by using Group Policy.

Apply local firewall rules: Not configured

Apply local connection security rules: Not configured

OK Cancel

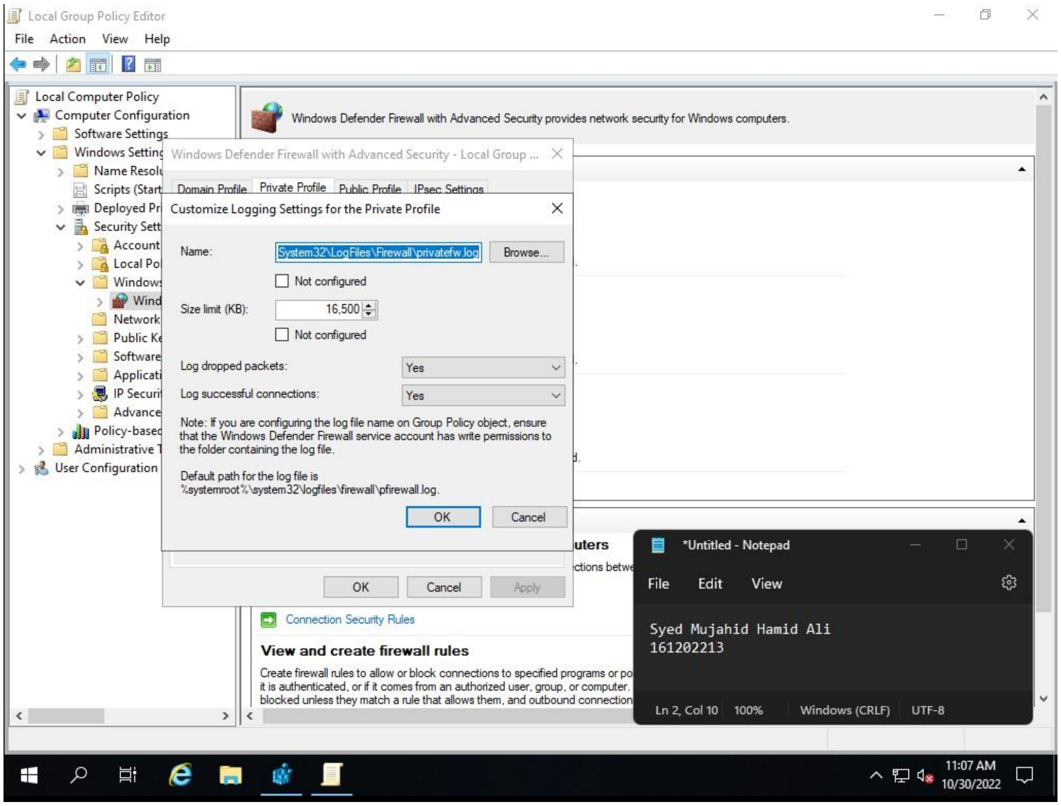
View and create firewall rules

Create firewall rules to allow or block connections to specified programs or po... it is authenticated, or if it comes from an authorized user, group, or computer. ... blocked unless they match a rule that allows them, and outbound connection...

*Untitled - Notepad

```
Syed Mujahid Hamid Ali
161202213
```

Ln 2, Col 10 100% Windows (CRLF) UTF-8



Windows Defender Firewall with Advanced Security provides network security for Windows computers.

Customize Logging Settings for the Private Profile

Name: System32\LogFiles\Firewall\privatefw.log Browse...

☐ Not configured

Size limit (KB): 16,500

☐ Not configured

Log dropped packets: Yes

Log successful connections: Yes

Note: If you are configuring the log file name on Group Policy object, ensure that the Windows Defender Firewall service account has write permissions to the folder containing the log file.

Default path for the log file is %systemroot%\system32\logfiles\firewall\pfirewall.log.

OK Cancel

OK Cancel Apply

View and create firewall rules

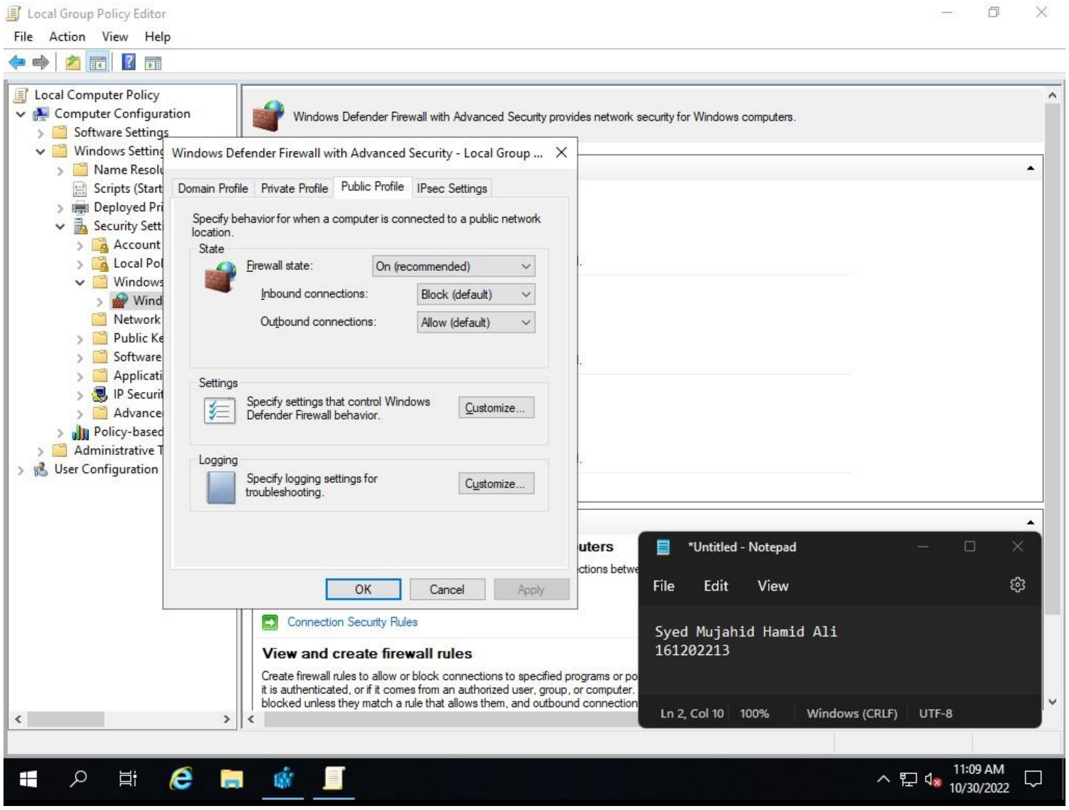
Create firewall rules to allow or block connections to specified programs or po it is authenticated, or if it comes from an authorized user, group, or computer. blocked unless they match a rule that allows them, and outbound connection

*Untitled - Notepad

```
Syed Mujahid Hamid Ali
161202213
```

Ln 2, Col 10 100% Windows (CRLF) UTF-8

The next one is to set the **Public Firewall** which contains policies that are majorly the same as the above two mentioned profiles.



Windows Defender Firewall with Advanced Security provides network security for Windows computers.

Windows Defender Firewall with Advanced Security - Local Group ...

Domain Profile | Private Profile | Public Profile | IPsec Settings

Specify behavior for when a computer is connected to a public network location.

State

Firewall state: On (recommended)

Inbound connections: Block (default)

Outbound connections: Allow (default)

Settings

Specify settings that control Windows Defender Firewall behavior. Customize...

Logging

Specify logging settings for troubleshooting. Customize...

OK Cancel Apply

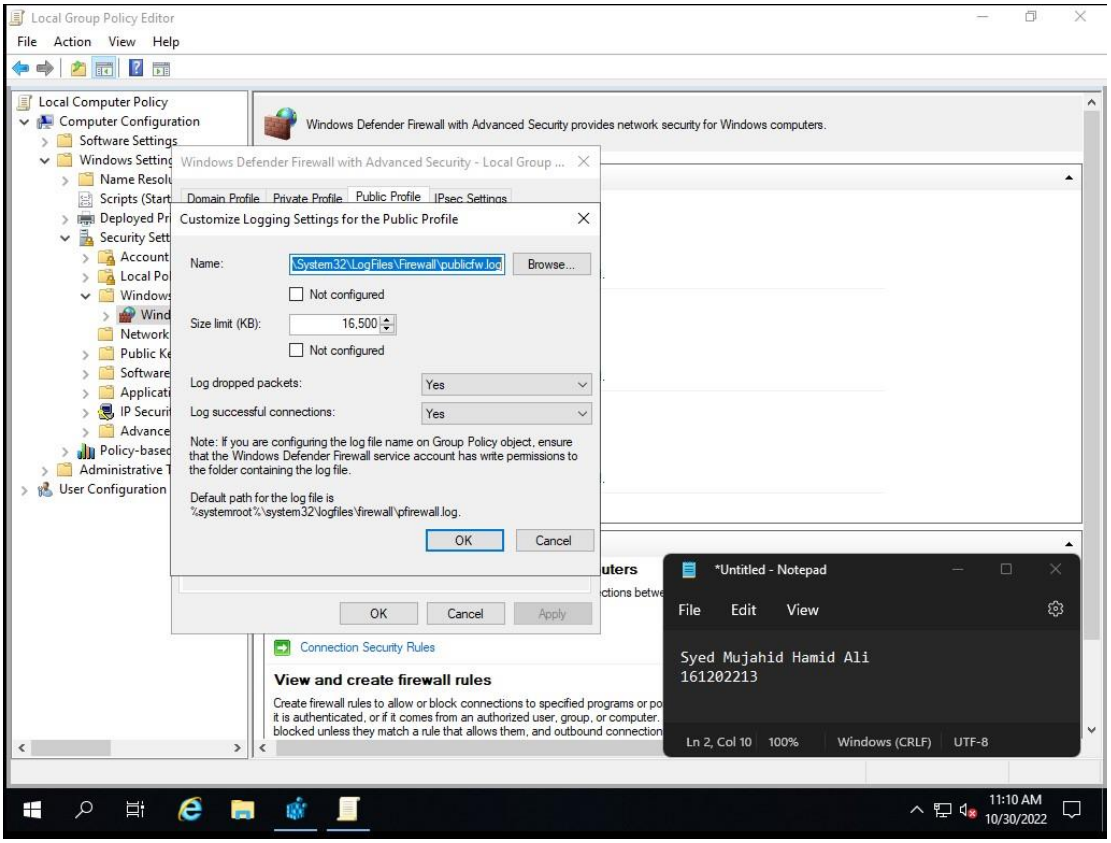
View and create firewall rules

Create firewall rules to allow or block connections to specified programs or po it is authenticated, or if it comes from an authorized user, group, or computer. blocked unless they match a rule that allows them, and outbound connection

*Untitled - Notepad

```
Syed Mujahid Hamid Ali
161202213
```

Ln 2, Col 10 100% Windows (CRLF) UTF-8



Windows Defender Firewall with Advanced Security provides network security for Windows computers.

Customize Logging Settings for the Public Profile

Name: \System32\LogFiles\Firewall\publicfw.log

☐ Not configured

Size limit (KB): 16,500

☐ Not configured

Log dropped packets: Yes

Log successful connections: Yes

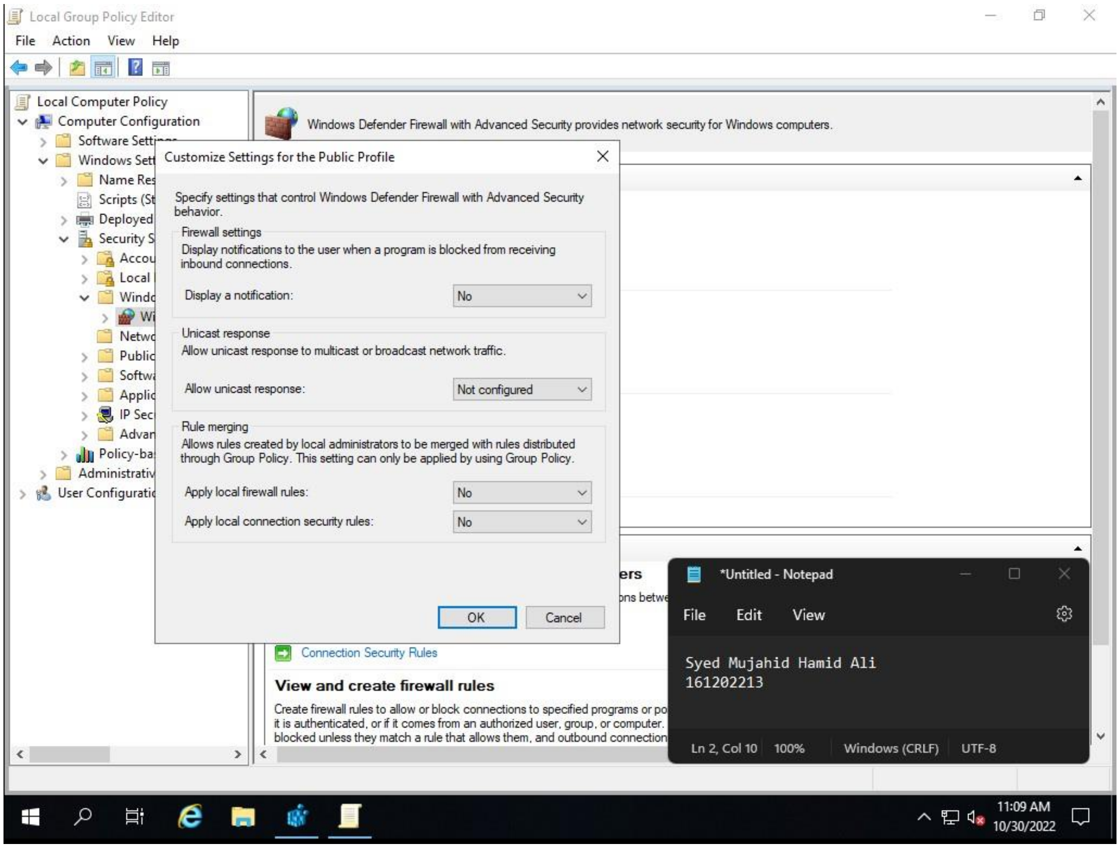
Note: If you are configuring the log file name on Group Policy object, ensure that the Windows Defender Firewall service account has write permissions to the folder containing the log file.

Default path for the log file is %systemroot%\system32\logfiles\firewall\pfirewall.log.

View and create firewall rules

Create firewall rules to allow or block connections to specified programs or po it is authenticated, or if it comes from an authorized user, group, or computer. blocked unless they match a rule that allows them, and outbound connection

```
Syed Mujahid Hamid Ali
161202213
```



Windows Defender Firewall with Advanced Security provides network security for Windows computers.

Customize Settings for the Public Profile

Specify settings that control Windows Defender Firewall with Advanced Security behavior.

Firewall settings

Display notifications to the user when a program is blocked from receiving inbound connections.

Display a notification: No

Unicast response

Allow unicast response to multicast or broadcast network traffic.

Allow unicast response: Not configured

Rule merging

Allows rules created by local administrators to be merged with rules distributed through Group Policy. This setting can only be applied by using Group Policy.

Apply local firewall rules: No

Apply local connection security rules: No

View and create firewall rules

Create firewall rules to allow or block connections to specified programs or po it is authenticated, or if it comes from an authorized user, group, or computer. blocked unless they match a rule that allows them, and outbound connection

```
Syed Mujahid Hamid Ali
161202213
```

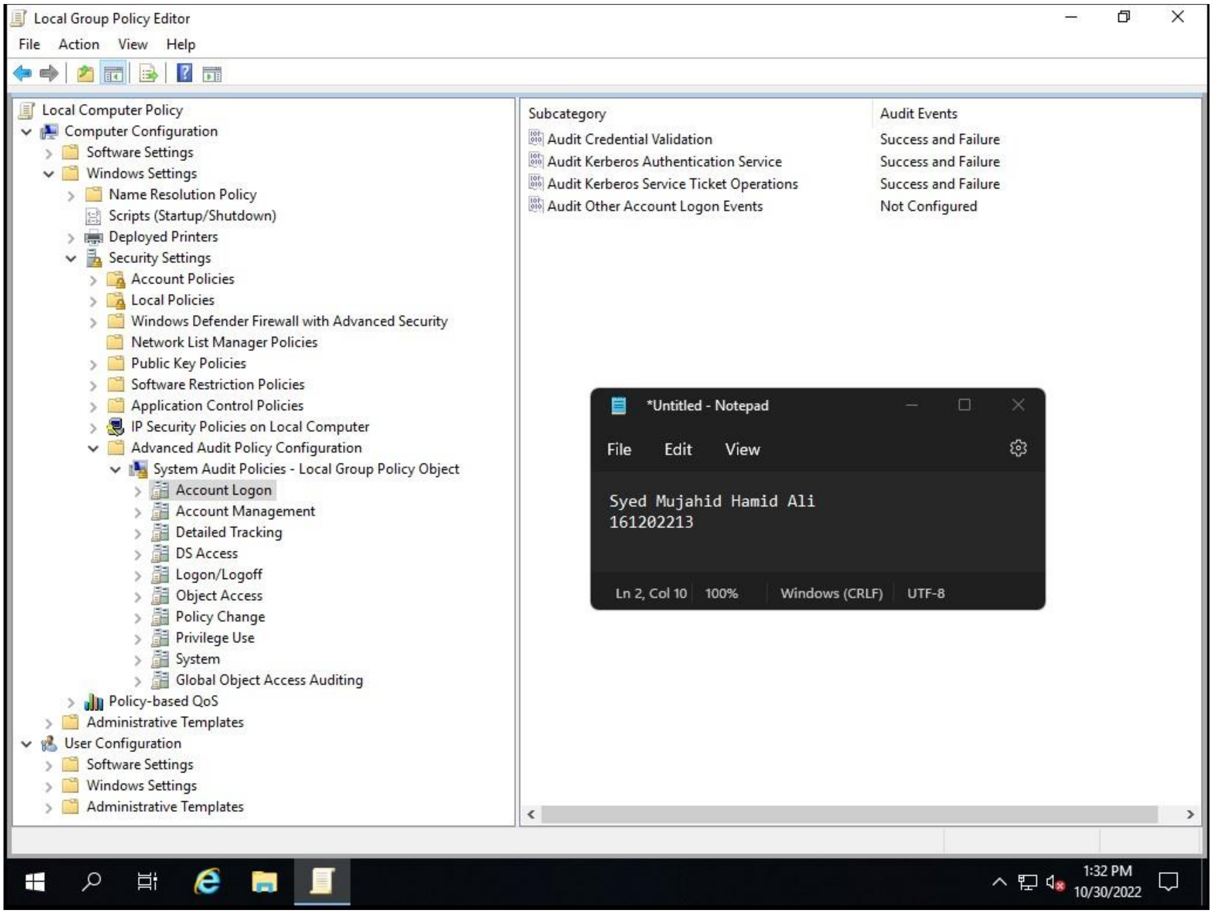
The next set of policies are made to configure the **<u>Advanced Audits</u>**.

The first one is for **<u>Account Logon</u>** configuration.

1. The first one is to ensure that Audit Credential Validation is set to Success and Failure because these records the results of validation tests made on the credentials of a user when they make a logon request. This is mainly helpful when they can be used for investigation a security incident.

2. The next one is to ensure that Audit Kerberos Authentication Service is also set to Success and Failure because this will report the results generated after a Kerberos authentication TGT request. Kerberos is an authentication service which allows clients to prove identity when they are running on behalf of a user. This is helpful because this will reduce the risk of an attacker trying to impersonate any user.

3. The next one is to set Audit Kerberos Service Ticket Operations as Success and Failure as well. This sub policy reports the results of events generated by ticket granting ticket (TGT) requests. This records the IP addresses from which account the above service was requested, when it was requested, and which type of encryption was used.



Subcategory	Audit Events
Audit Credential Validation	Success and Failure
Audit Kerberos Authentication Service	Success and Failure
Audit Kerberos Service Ticket Operations	Success and Failure
Audit Other Account Logon Events	Not Configured

*Untitled - Notepad

Syed Mujahid Hamid Ali
161202213

The next part is to set policies for **Account Management**.

1. The first one is to ensure that Audit Application Group Management is set to Success and Failure. This allows us to audit events generated by changes made to the application groups like creating or removing a group or even a member from a group. If this not set properly, then some of the security incidents might not be detected. Another case would be that there would be very less evidence for analyzing a security incident if any takes place.

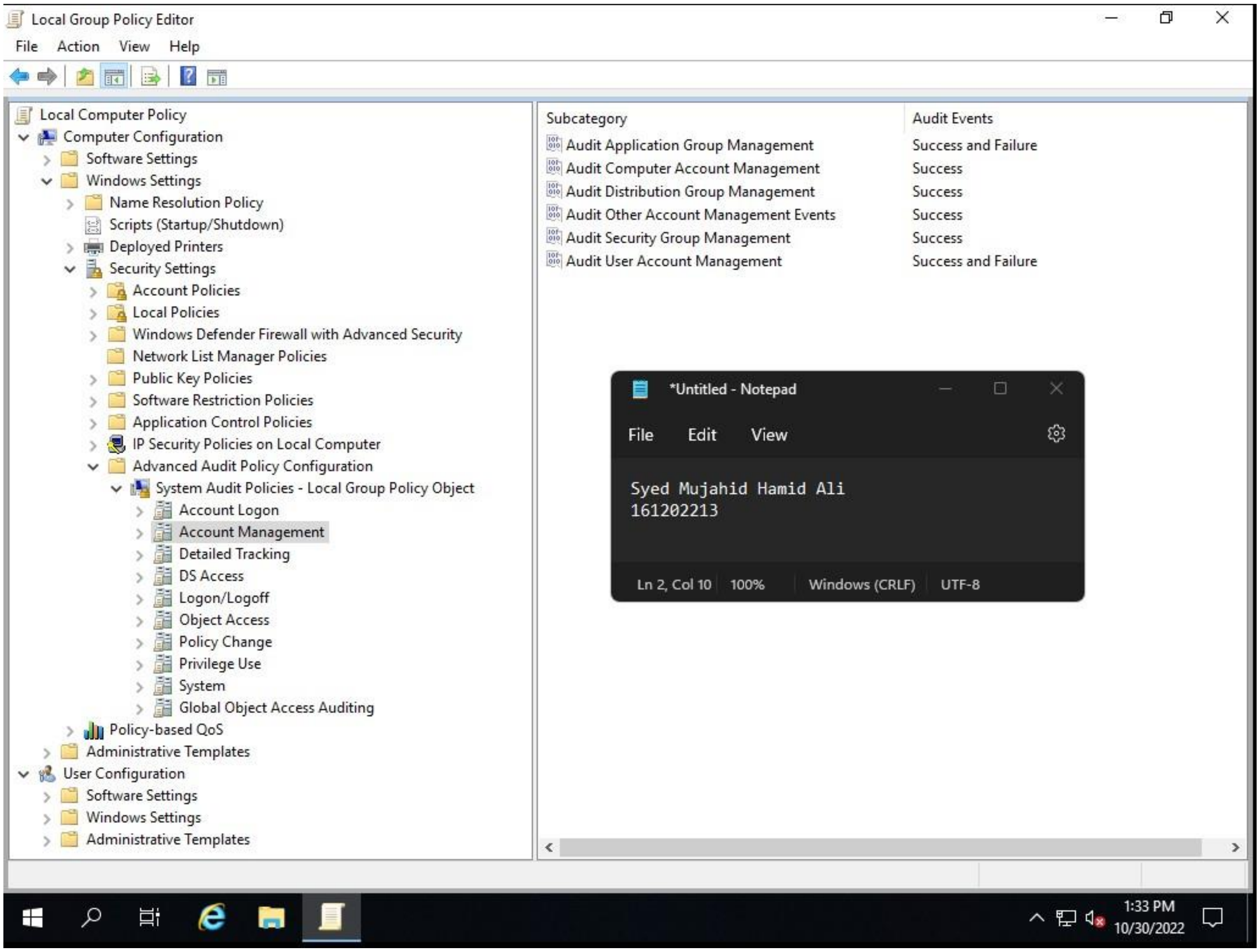
2. The next one is to set Audit Computer Account Management as only Success. This will only report the events made in the computer account management such as an account was created, changed, or deleted. If this is not configured at all, then this would result in calamities mentioned for above.

3. The next one is to ensure that Audit Distribution Group Management is set to only success. This policy reports each event of distribution group management, like when a group is changed or removed, or even if a member is added or removed from a group. This will allow administrators to track events that will enable to detect any sort of suspicious or wrongful creation of groups.

4. The next one is to ensure that Audit Other Account Management Events is set to only success. This is done because this will record any other events that took place in the account management like if a password hash was accessed.

5. The next one is to ensure that Audit Security Group Management is set to success only. This subcategory reports each event of security group management like creation or deletion of security groups or when a user is added or removed from any group. This will also help administrators to track events when any wrongful groups were created.

6. The next one is to ensure that Audit User Account Management is set to both Success and Failure because this allows us to report any event that takes place in the user account management like creation od deletion of user and it also includes changing of passwords.



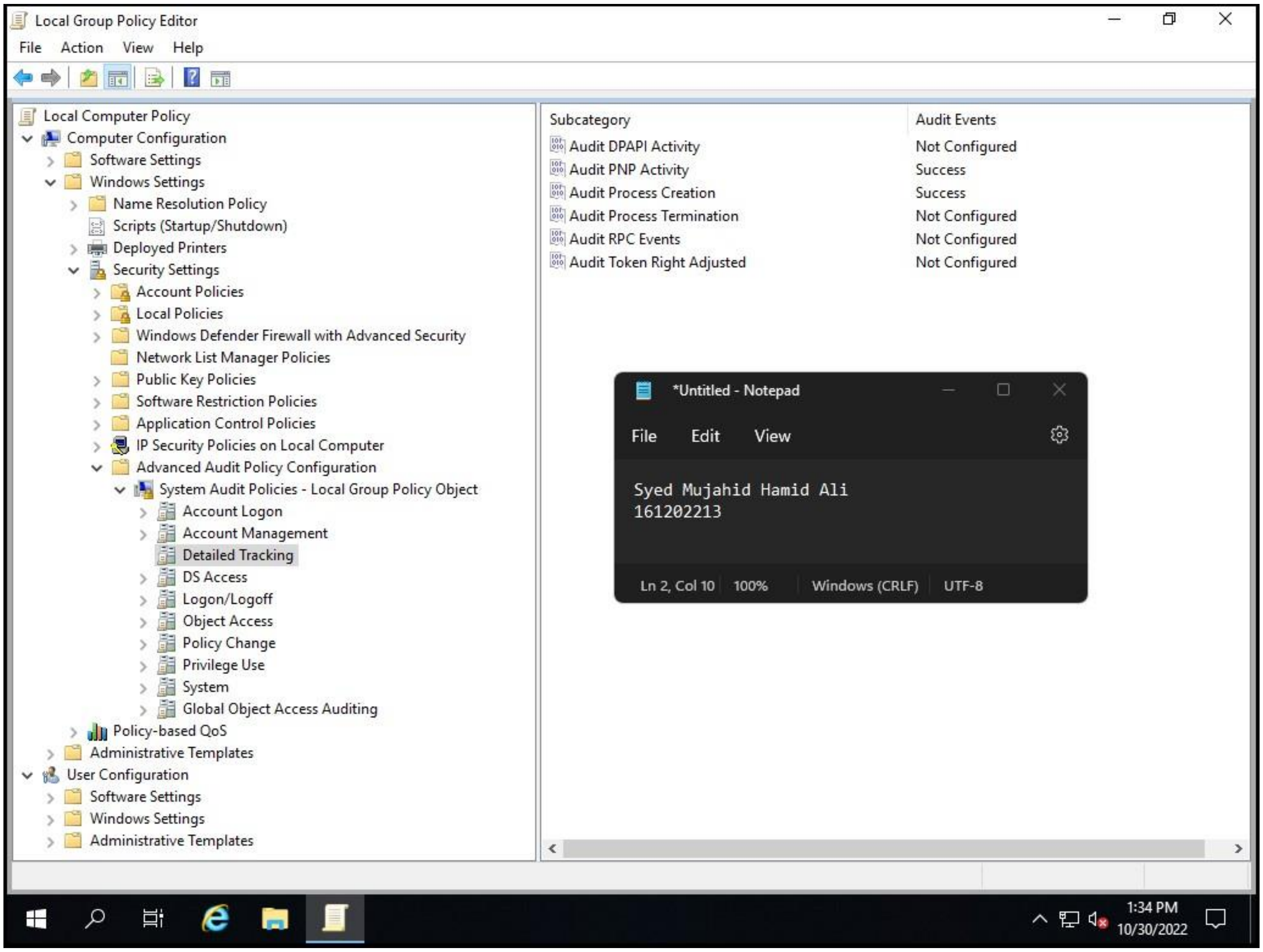
Subcategory	Audit Events
Audit Application Group Management	Success and Failure
Audit Computer Account Management	Success
Audit Distribution Group Management	Success
Audit Other Account Management Events	Success
Audit Security Group Management	Success
Audit User Account Management	Success and Failure

```
Syed Mujahid Hamid Ali
161202213
```

The next part is to set policies for **Detailed Tracking**.

1. The first one is to ensure that Audit PNP Activity is set to Success only. This is because this setting allows us to audit when plug and play (PNP) detects any external device. This is useful when the IT staff gets alerted if an unapproved device is plugged in.

2. The next one is to ensure that Audit Process Creation is set to only Success because this setting allows us to audit and report the creation of any process with the name of the program and the user that created it.



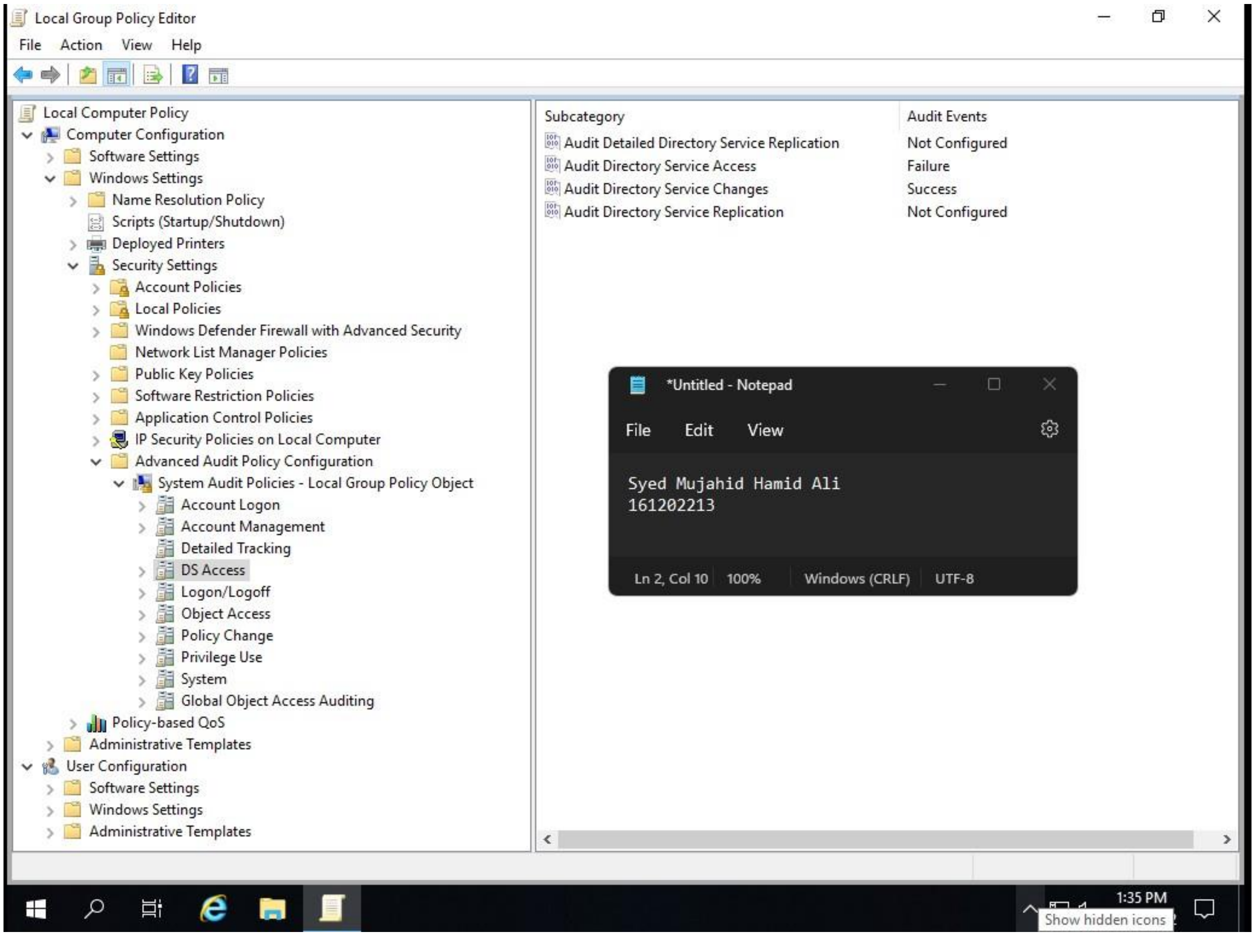
Subcategory	Audit Events
Audit DPAPI Activity	Not Configured
Audit PNP Activity	Success
Audit Process Creation	Success
Audit Process Termination	Not Configured
Audit RPC Events	Not Configured
Audit Token Right Adjusted	Not Configured

```
Syed Mujahid Hamid Ali
161202213
```

The next part is to follow the recommendations for **DS (Directory Service) Access**.

1. The first one is to ensure that Audit Directory Service Access is set to only Failure because this allows us to report when an object is accessed from the active directory (AD). This can also be helpful when analyzing a security incident if any that took place.

2. The next one is to set the Audit Directory Service Changes is set to only Success because this will report the changes that are made to the objects present inside the active directory. These include creating, modifying, or even moving any object from AD. If not configured properly, security incidents might not be detected which could have been useful when analyzing a security incident.



Subcategory	Audit Events
Audit Detailed Directory Service Replication	Not Configured
Audit Directory Service Access	Failure
Audit Directory Service Changes	Success
Audit Directory Service Replication	Not Configured

```
Syed Mujahid Hamid Ali
161202213
```

The next one to follow the recommendations for configuring the **Logon/Logoff Audit Policy**.

1. The first one is to ensure that Audit Account Lockout is set to only Failure because this reports when a user account is locked due too many failed login attempts. If this is not configured properly, then these changes will not be recorded or reported, which could be useful if any security incident took place.

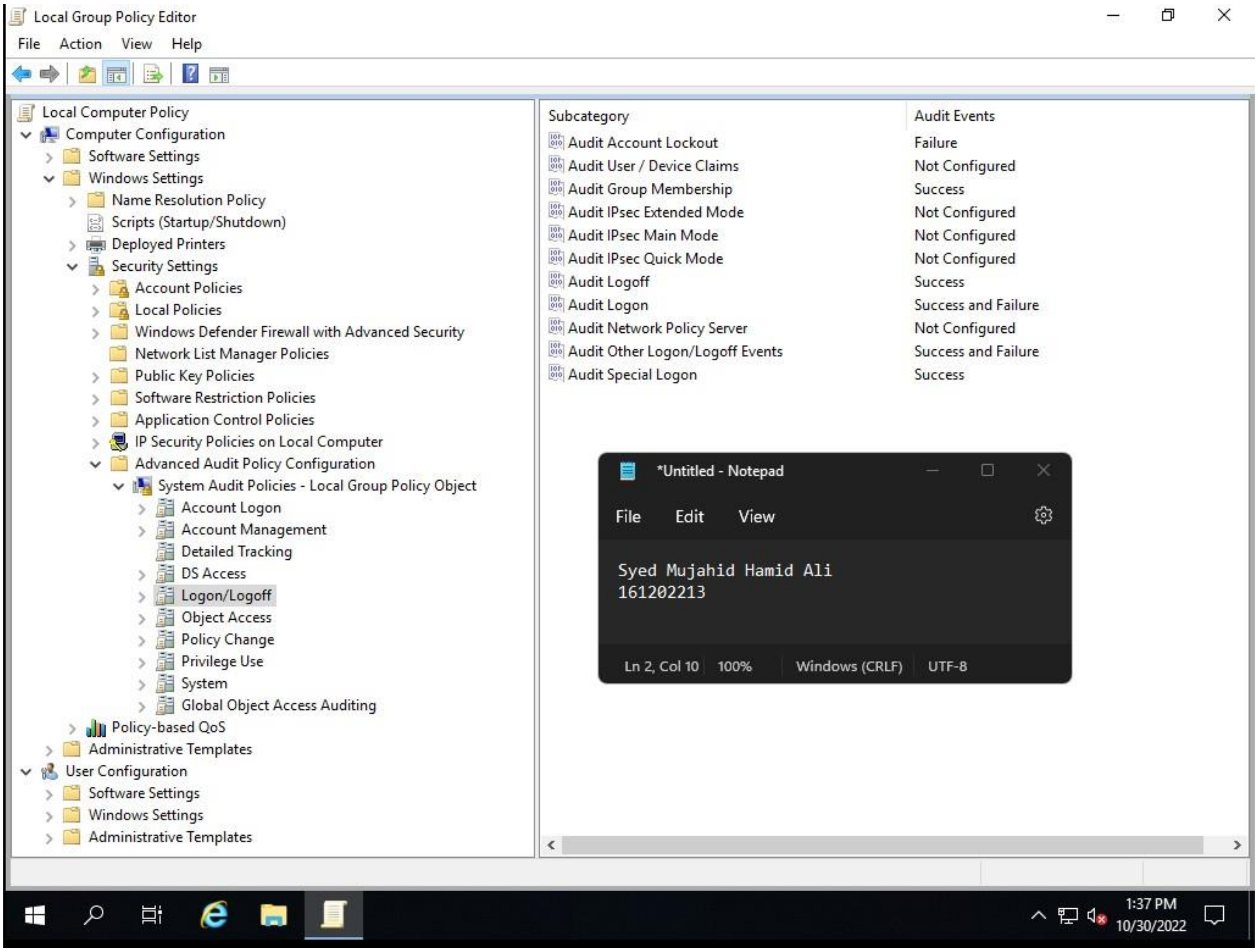
2. The next one is to ensure that Audit Group Membership is set to only Success because this policy allows us to audit the group membership data in the login token created by the user and documenting these events can be useful when investigating security incidents if any take place.

3. The next one is to set Audit Logoff to only Success because this will report whenever a user logs off from the system. If not configured properly then it becomes almost impossible to determine which user has attempted to access the organization’s computers.

4. Next one is to set Audit Logon to as both Success and Failure. This is because this subcategory will report whenever a user logs in to the system. These can be very helpful when investigating any security incident that took place.

5. The recommendation given for the next subcategory is to set Audit Other Logon/Logoff Events as both Success and Failure because this will report both login and logoff events like remote desktop service. This can be very helpful when analyzing and investigating security incidents that took place in the organisation.

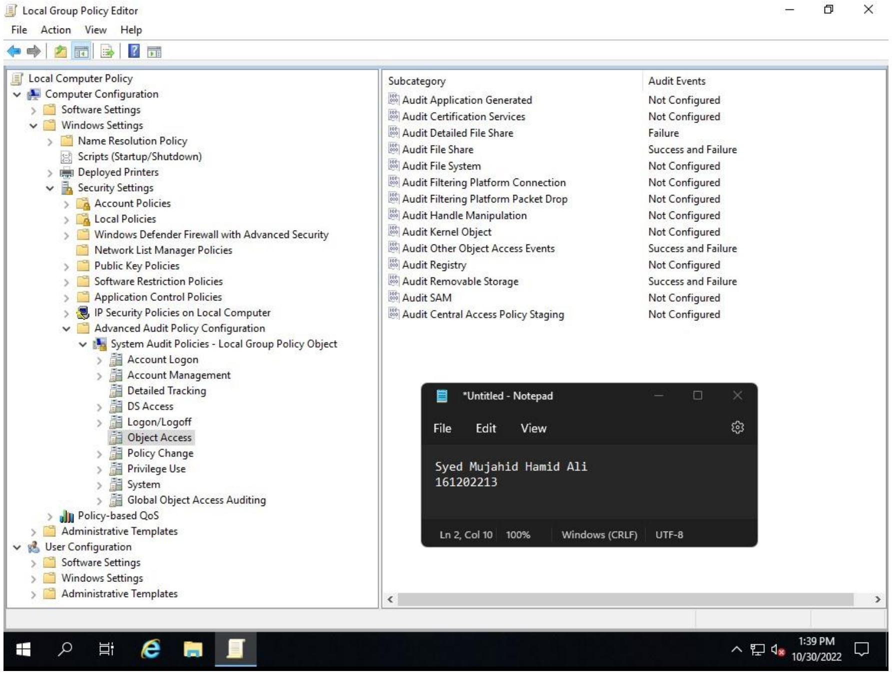
6. The last one for this section is to set Audit Special Logon is set to only success because this reports when a special logon is used. A special logon means that an account with special privileges like an administrator was used to increase the priority of a process to a higher level. If this is not configured properly, an attacker can log in and elevate the priority of a malicious process which could kill other critical processes and the end, we will have no proof whatsoever that this all happened.



Subcategory	Audit Events
Audit Account Lockout	Failure
Audit User / Device Claims	Not Configured
Audit Group Membership	Success
Audit IPsec Extended Mode	Not Configured
Audit IPsec Main Mode	Not Configured
Audit IPsec Quick Mode	Not Configured
Audit Logoff	Success
Audit Logon	Success and Failure
Audit Network Policy Server	Not Configured
Audit Other Logon/Logoff Events	Success and Failure
Audit Special Logon	Success

```
Syed Mujahid Hamid Ali
161202213
```

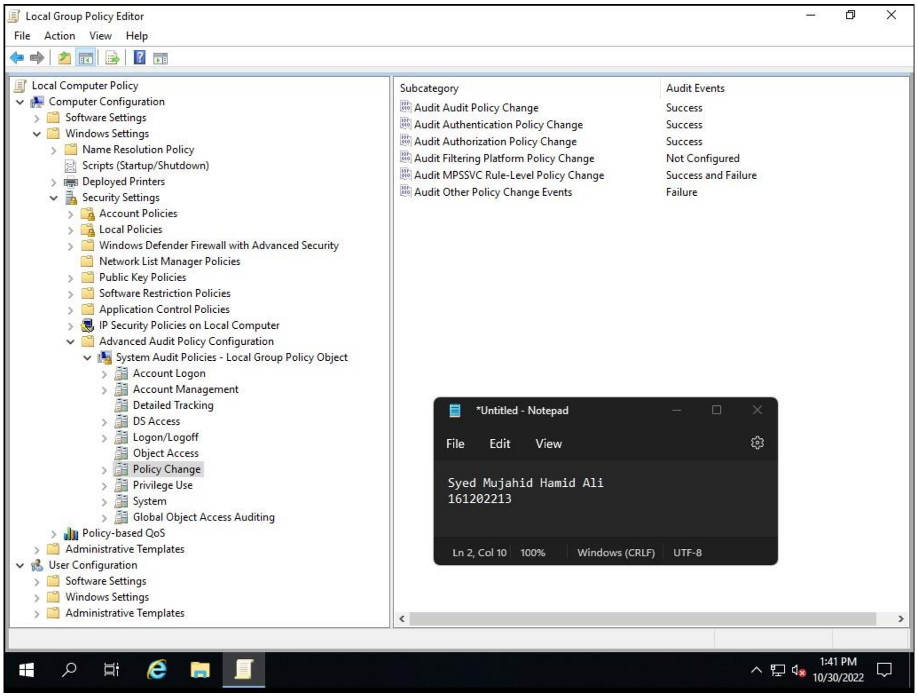
The next section contains recommendations for configuring the **Object Access Audit Policy**. Like the above sections, there are many policies that can be used while analyzing and investigating security incidents if any take place.



Subcategory	Audit Events
Audit Application Generated	Not Configured
Audit Certification Services	Not Configured
Audit Detailed File Share	Failure
Audit File Share	Success and Failure
Audit File System	Not Configured
Audit Filtering Platform Connection	Not Configured
Audit Filtering Platform Packet Drop	Not Configured
Audit Handle Manipulation	Not Configured
Audit Kernel Object	Not Configured
Audit Other Object Access Events	Success and Failure
Audit Registry	Not Configured
Audit Removable Storage	Success and Failure
Audit SAM	Not Configured
Audit Central Access Policy Staging	Not Configured

```
Syed Mujahid Hamid Ali
161202213
```

The next section contains recommendations for configuring the **Policy Change Audit Policy.** This also contains recommendations that are like the ones above.

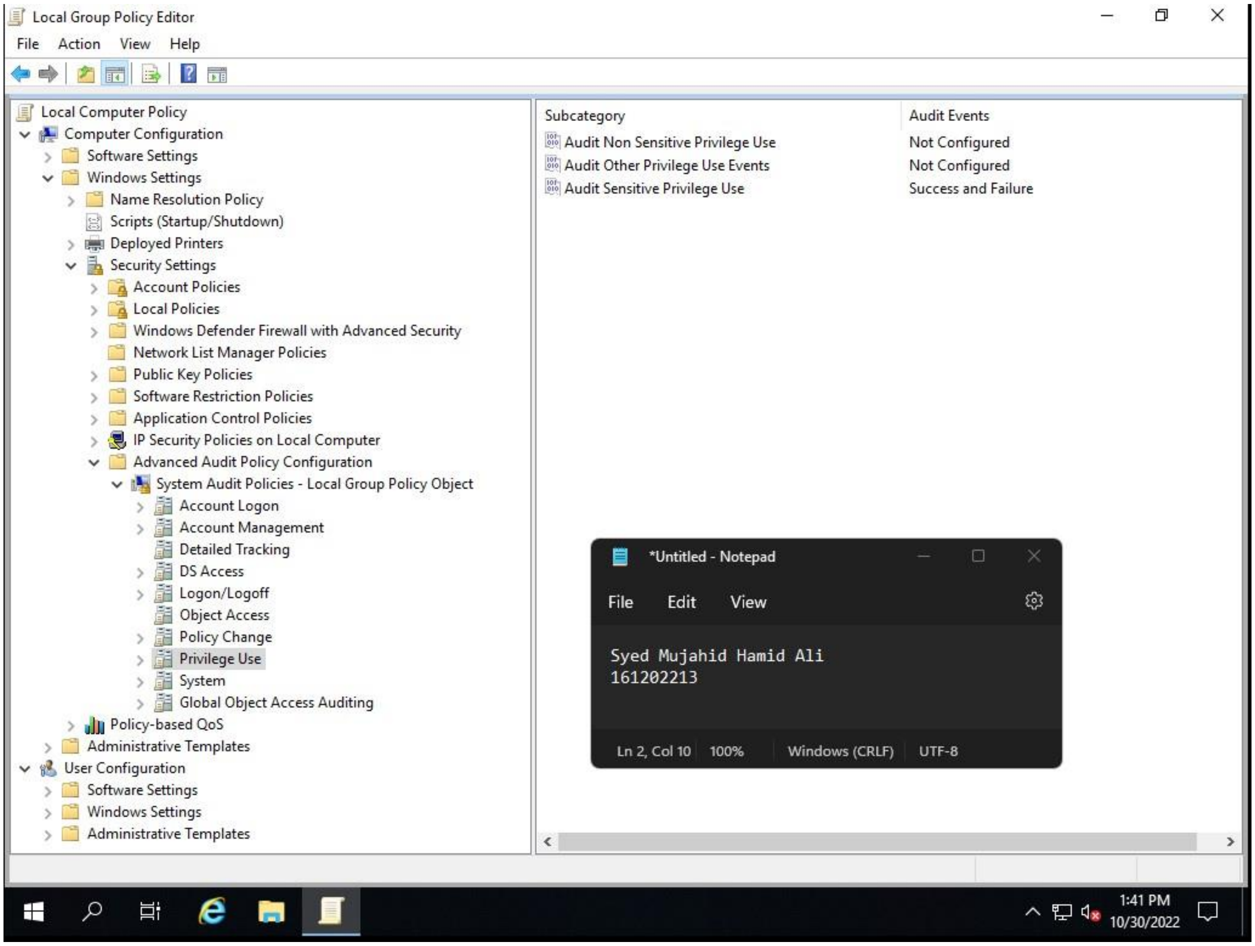


Subcategory	Audit Events
Audit Audit Policy Change	Success
Audit Authentication Policy Change	Success
Audit Authorization Policy Change	Success
Audit Filtering Platform Policy Change	Not Configured
Audit MPSSVC Rule-Level Policy Change	Success and Failure
Audit Other Policy Change Events	Failure

```
Syed Mujahid Hamid Ali
161202213
```

The next part includes recommendations for implementing the **<u>Privilege Use Audit Policy</u>**.

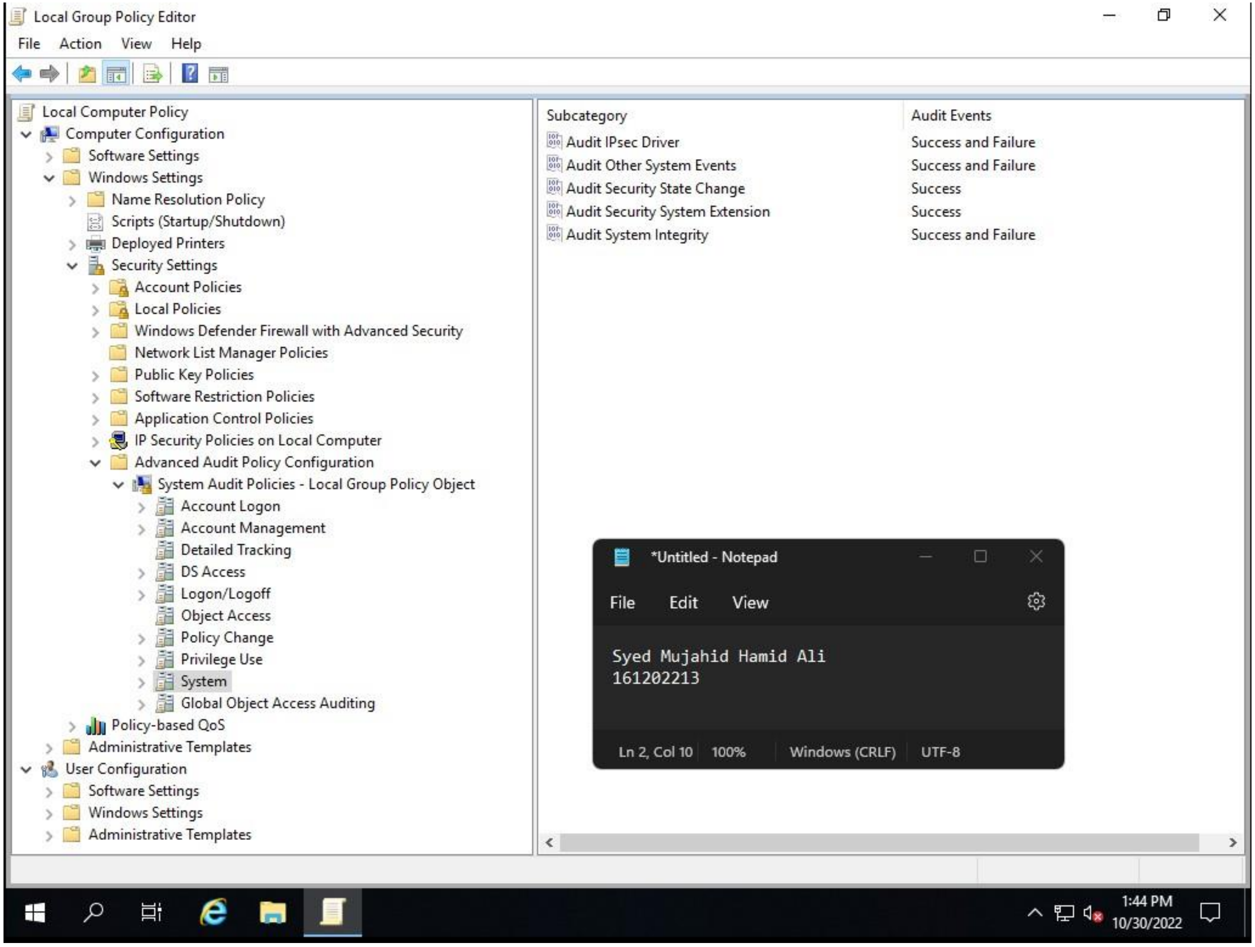
1. There is only category in this, and we must ensure that Audit Sensitive Privilege Use is set to both Success and Failure. This is because this allows us to report when an account or service uses sensitive privileges like backing up files or directories, creating token, debugging, etc. Auditing these events will include information like when and by whom the service was called, which may be useful when investigating a security incident.



Subcategory	Audit Events
Audit Non Sensitive Privilege Use	Not Configured
Audit Other Privilege Use Events	Not Configured
Audit Sensitive Privilege Use	Success and Failure

```
Syed Mujahid Hamid Ali
161202213
```

The last section has the recommendations for configuring the **System Audit Policy**.



Subcategory	Audit Events
Audit IPsec Driver	Success and Failure
Audit Other System Events	Success and Failure
Audit Security State Change	Success
Audit Security System Extension	Success
Audit System Integrity	Success and Failure

```
Syed Mujahid Hamid Ali
161202213
```

Description of how it can be tested

There are multiple ways to test these different policies that we just implemented. The most worth mentioning would be:

1. We could check if our password polices are put in place and are being implemented by creating a user account and setting a password which would contradict the policies. This way if it can set the password, that means the policies are not being implemented at all.

2. To check the firewall policy, we can try simulating an attacker's perspective by untrusting a known network and trying to connect to our system. This way if it connects, we will be able to know that there is something wrong with our inbound connection settings.

3. To check the audits, we can open and check what all has been documented from time to time like monthly maybe. If we notice that something has been missed out, we could further process an event that we might think could be something that was missed out and see if it still does not get audited. This way we will come to know that something is wrong with our audit policy configurations.