Lab Report 9

1. Assessment Sheet
2. **What is the main difference between a virus and a Trojan？**

Trojan House will disguise them and cheat victims out of running them and it cannot reproduce; otherwise, a virus can reproduce and infect more computers which connected with an infected computer.

1. **A virus or malware can impact which of the three tenets of information systems security (Confidentiality, integrity, availability)? In what way?**

The virus and malware will compromise all the three aspects, Confidentiality, integrity and availability, of information system. A virus can gain system controls, which bypass the access control. This is the compromise of confidentiality. For integrity, the malicious software could change the content of the data, destroy the data. And, for availability, take worms as an example, it will reproduce by them and exhaust the system resources which can prevent the computer form providing services to end user.

1. **Why is it recommended to do an antivirus signature file update before performing an antivirus scan on your computer?**

The virus changes day by day and the signature file are relatively static. As a result, if we don’t upgrade the signature file frequently, we could not prevent the latest virus which might cause huge losses.

1. **Why might your coworker suggest encrypting an archive file before e-mailing it?**

The reason is that the antivirus tools cannot scan an encrypted file so that the staff can take advantage of this bypassing the security check.

1. **What kind of network traffic can you filter with the Windows Firewall with Advanced Security?**

In the windows Firewall advanced security settings, we could enable numerous rules which all are classified as two categories – Inbound Rules and Outbound Rules. And for the network traffic, it has a category which name is start with Core Networking or Network which helps us to block any unwanted network traffics such as preventing specific http request from receiving and responding.

1. **What are typical indicators that your computer system is compromised？**

There are several symptoms which show that our computer system is compromised.

* System performance decreased day by day
* Applications behave abnormally
* System log and application show abnormal records.

1. **What elements are needed in a workstation domain policy regarding use of antivirus and malicious software prevention tools?**

In my option, the domain policy should contain following elements

* Real-time protection – allow anti-virus run in background
* Update virus signature database frequently
* Periodically scan the system through anti-virus tools

1. Challenge Questions

**Description: 1) Encrypted files cannot be inspected by an anti-virus program. Explain your answer. 2) Research best practices for handling archive files in a network environment and make recommendations for ensuring integrity of the data stored on the network. 3) Research Windows services. Using the screen capture in Part 2 of the lab, identify at least three services that could be disabled safely. Explain your choices**

Answer for 1st question:

It is true that anti-virus tool could not detected viruses which reside in an encrypted file because anti-virus tools doesn’t have the ability to crack the password and also according to the working principle of these kinds of tools, they could not detect virus unless they can directly load the file in memory. So, if a file is encrypted, the content could not load in memory and as a result, the anti-virus tools fail to work as expected on encrypted file.

Answer for 2nd question:

Actually, we cannot direct inspect a archived file but what we can do is to run the anti-virus in the background and once the user unzip that archive file, the anti-virus should start a quick scan of that file before user see the decompressing result.

Answer for 3rd question:

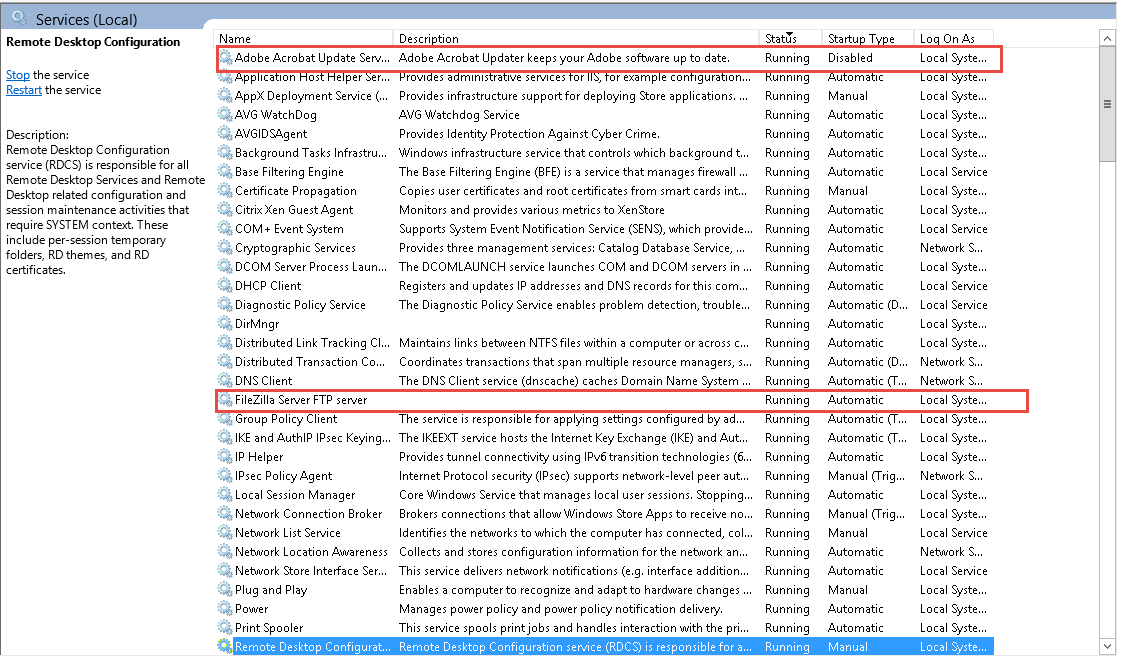
According to my research, I think the following services are not required in Vworkstation

1. Adobe Acrobat Update Service

This service is used to monitor the Adobe Acrobat products with the latest released updates on these products automatically and it will automatically download and install latest patches and updates. However, it not necessary for the Vworkstation to enable this services, we can manually patch and update those products.

1. FileZilla Server FTP server

This service is run by FileZillar software, which is a tool used to transmit files between clients and servers. As my observation, we have seldom opportunities to use this functionality in Vworkstation. So, we could disable this service. In addition, the FTP services are always a dangerous threat for information systems because they are easily attacked.

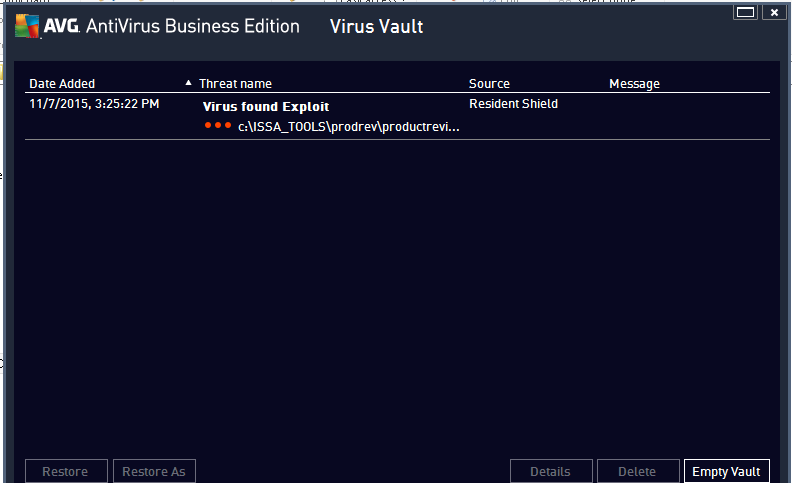


1. Themes services

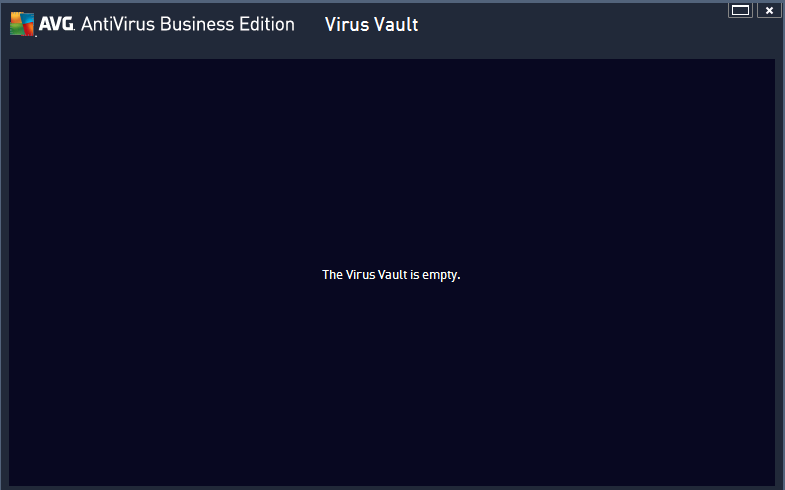
Themes service is used to enhance user experience and it is not necessary to run it because in Vworkstation we don’t have high requirement on user experience.



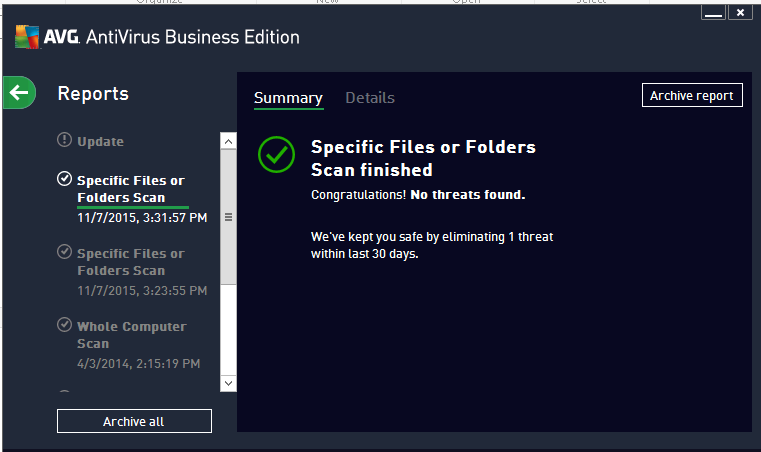
1. Report Screenshot
2. AVG Virus Vault



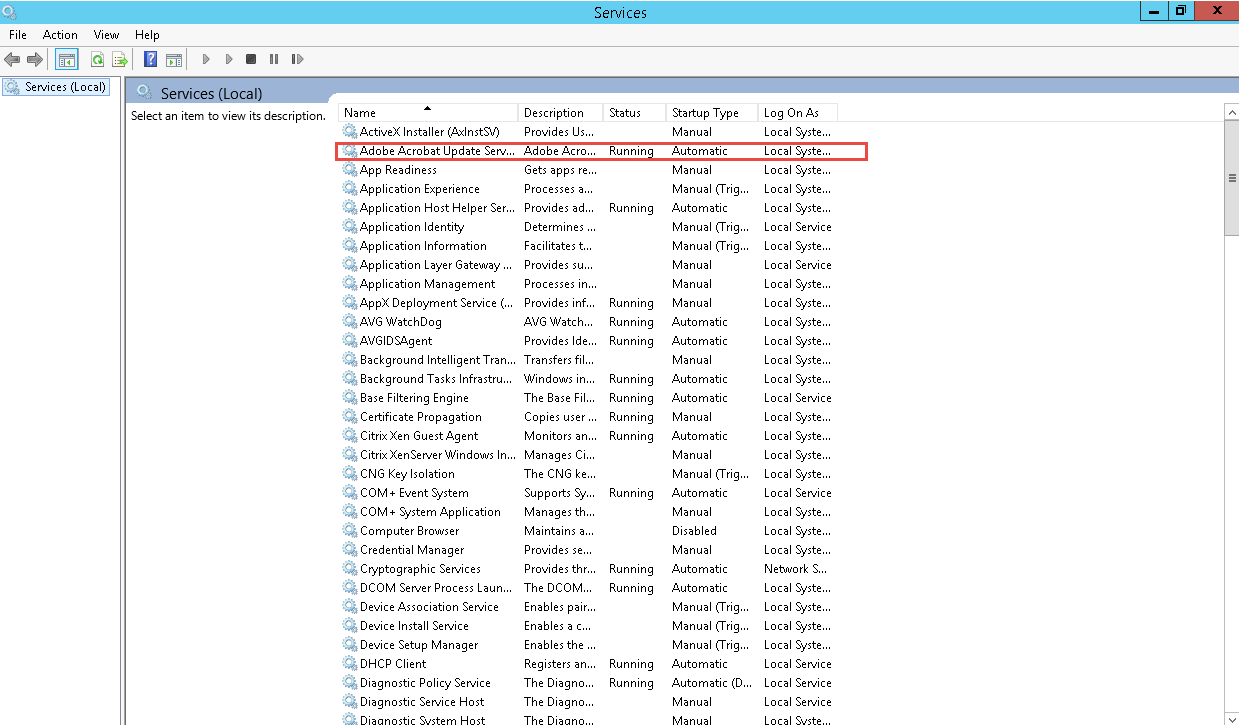
1. AVG Empty Virus Vault

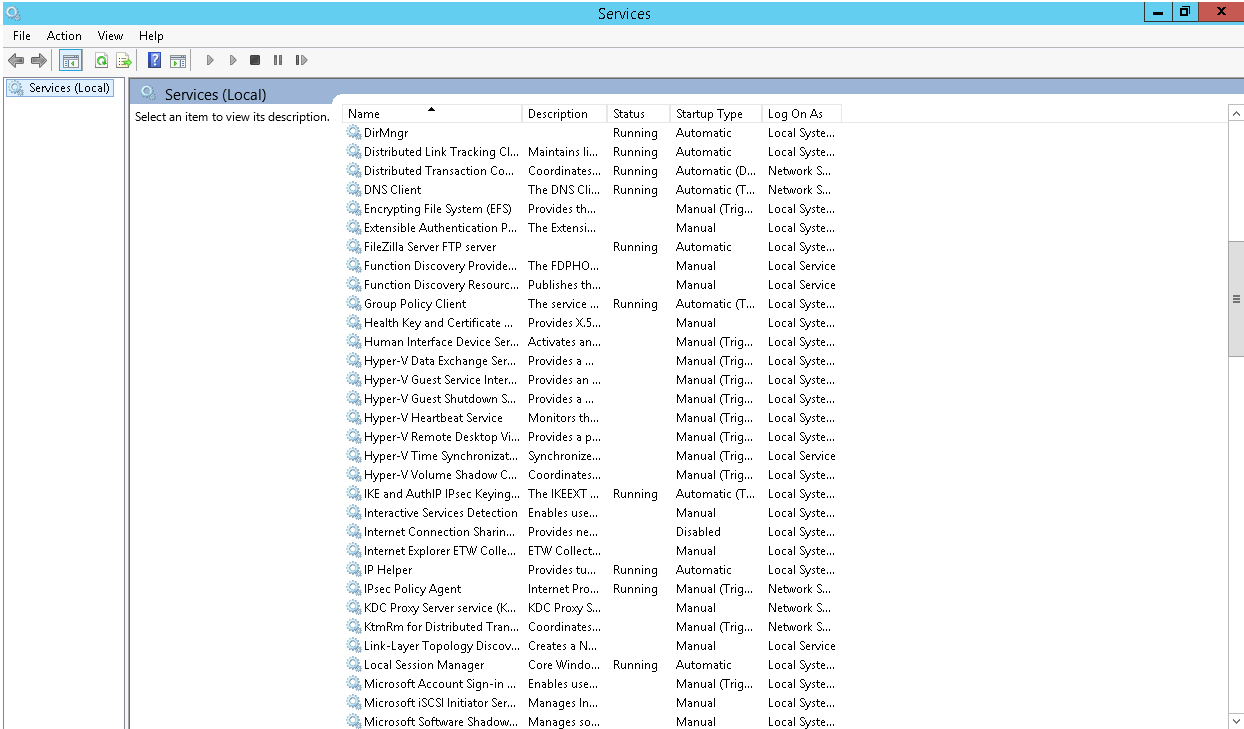


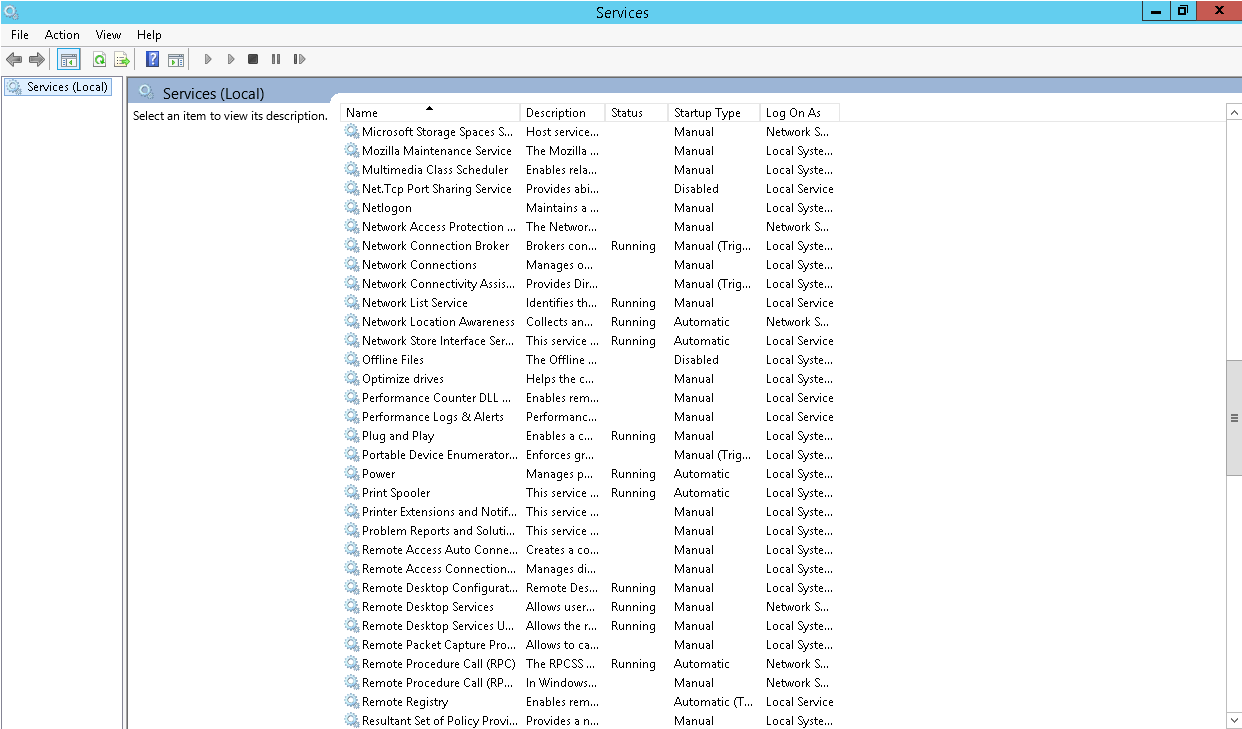
1. AVG second scan result

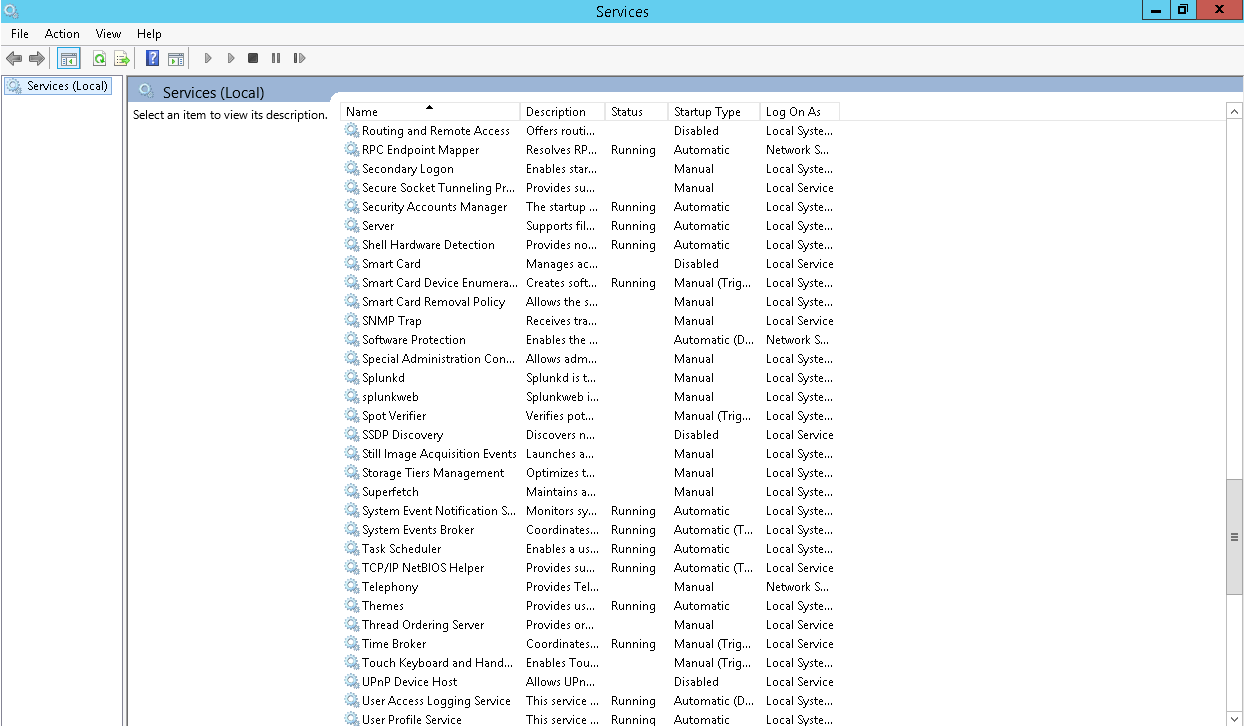


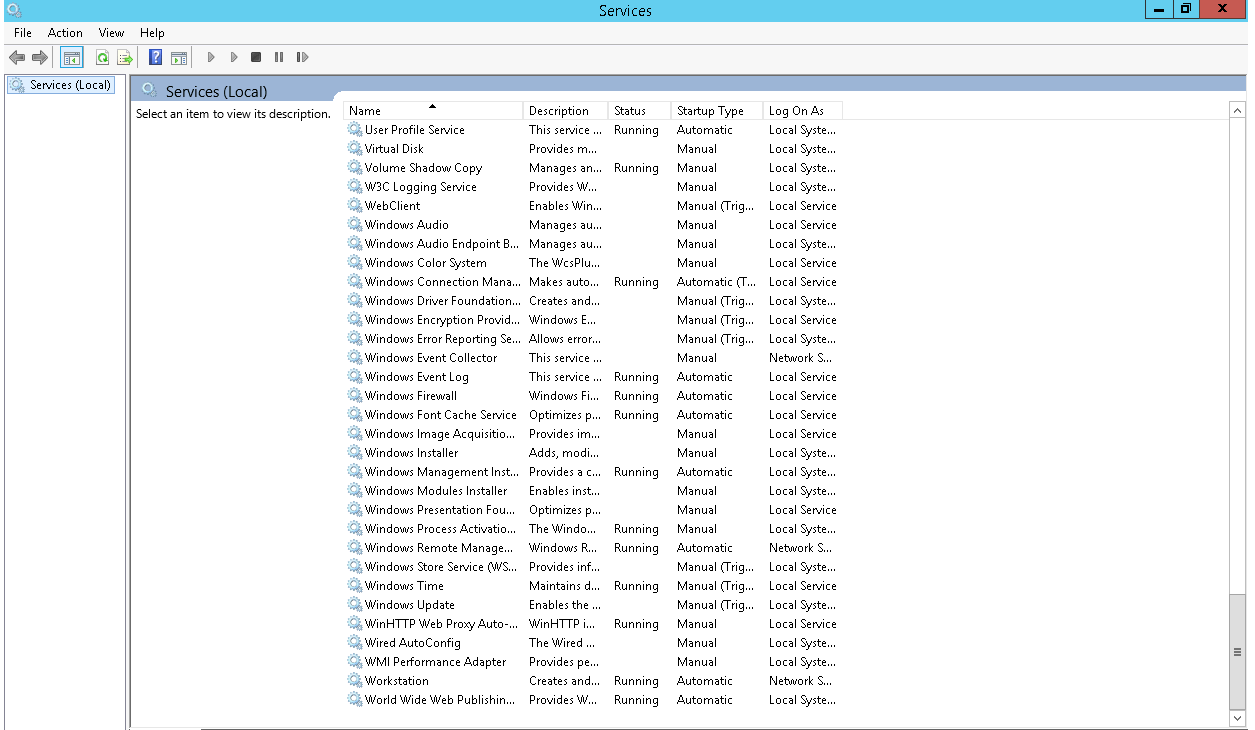
1. Complete list of services running on Vworkstation



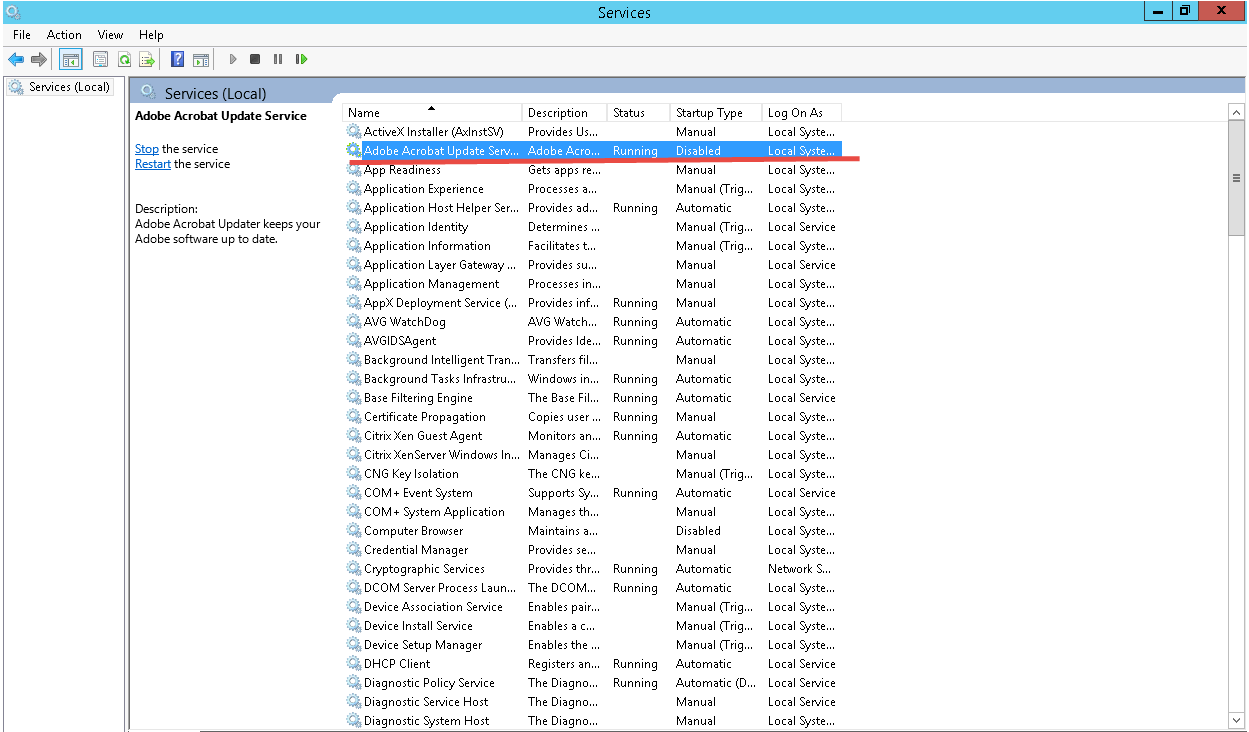




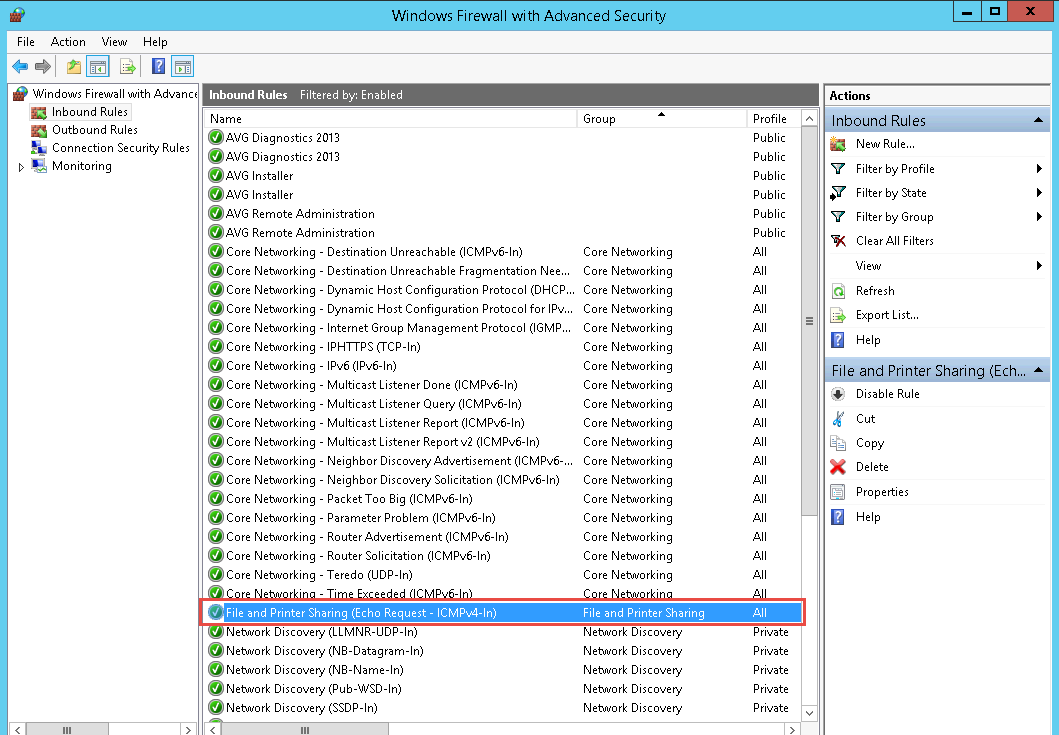




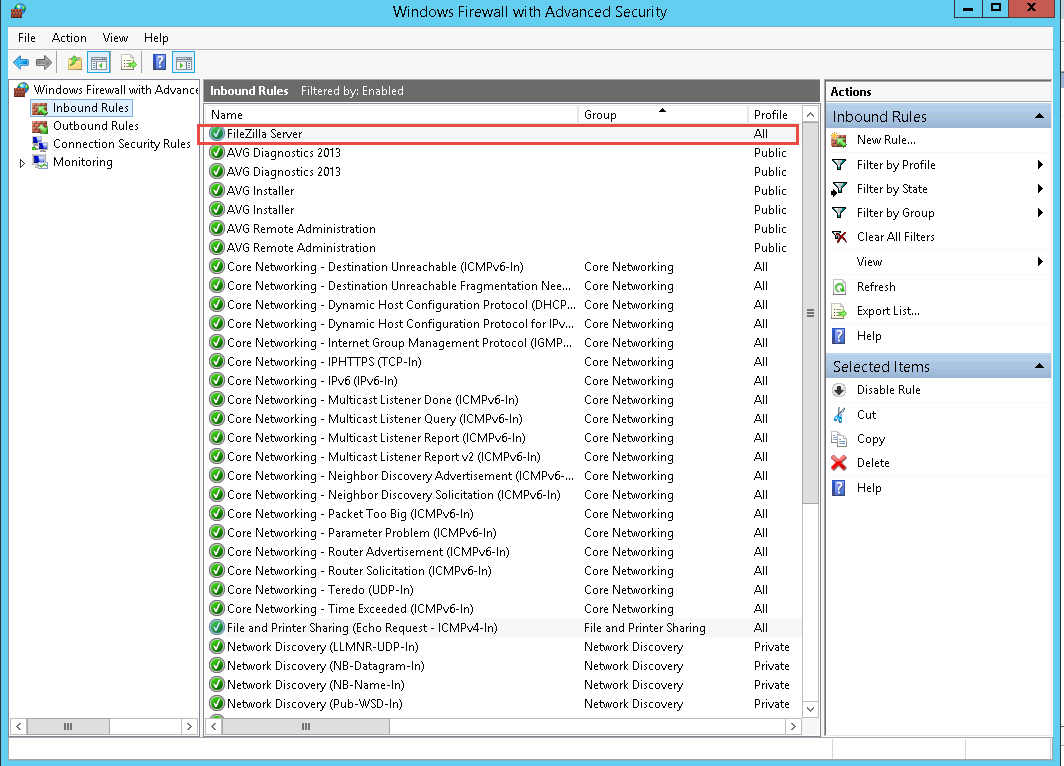
1. Updated list of services of Adobe acrobat update



1. Enable File and Printer Sharing rule



1. New FileZilla Server rules



1. Other additional supporting text/image content

Lab Report 10

1. Assessment Sheet
2. **What is the correct command syntax to force GPO settings?**
3. /force GPO
4. gpupdate /now
5. gpupdate /force
6. policyupdate /force

Answer: C

1. **Why is it important to set a strict password policy as part of your security template?**

If we set a strict password policy, we can deter the hackers to crack the password both from social engineer approach and technical approach.

1. **Why is it important to bring standalone systems into the Domain?**

As a standalone system, it not easy for administrator to manage because if there is 1 standalone system, the administrator can set up policy particularly, but if there are 1000+ systems, the administrator could not set up individually. But if we incorporate these systems into a Domain, we can set up policies controls at a high level instead of setting up computer by computer.

1. **What was the command line syntax to connect as the root user to 172.30.0.11 using putty**

putty [root@172.30.0.11](mailto:root@172.30.0.11) –pw toor

1. **Name five different Windows password policies**

Enforce password history

Maximum password age

Minimum password length

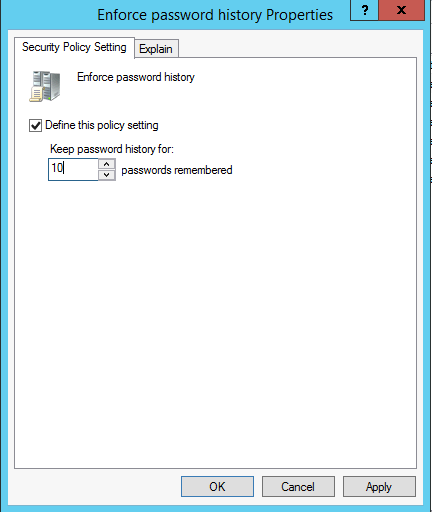
Password must meet complexity requirements

Minimum password age

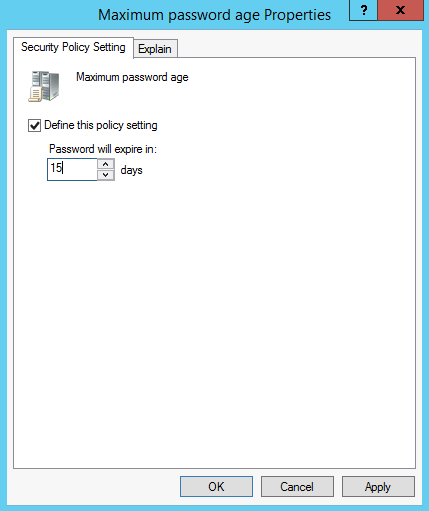
1. Challenge Questions

**Description: Document the changes of default domain controller which meets 1) users may not reuse the last 10 password;2) users must change passwords every 15 days; 3) Passwords may be reset at any time; 4) Passwords must be a minimum of 12 characters; 5) Enforce basic password complexity; 6) Default Domain Policy should not override the settings of Default Domain controller**

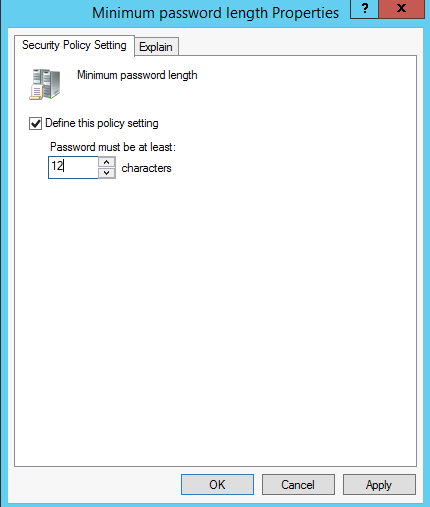
1. Users cannot reuse the last 10 password



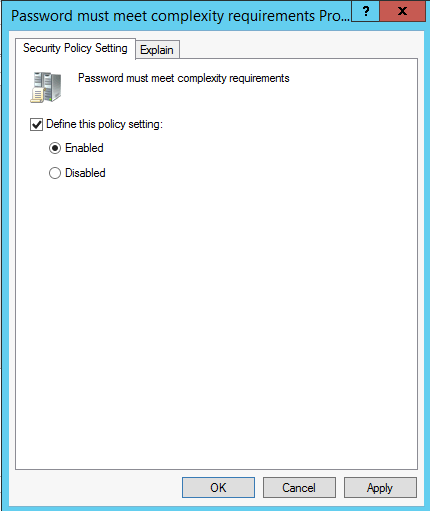
1. Change password every 15 days



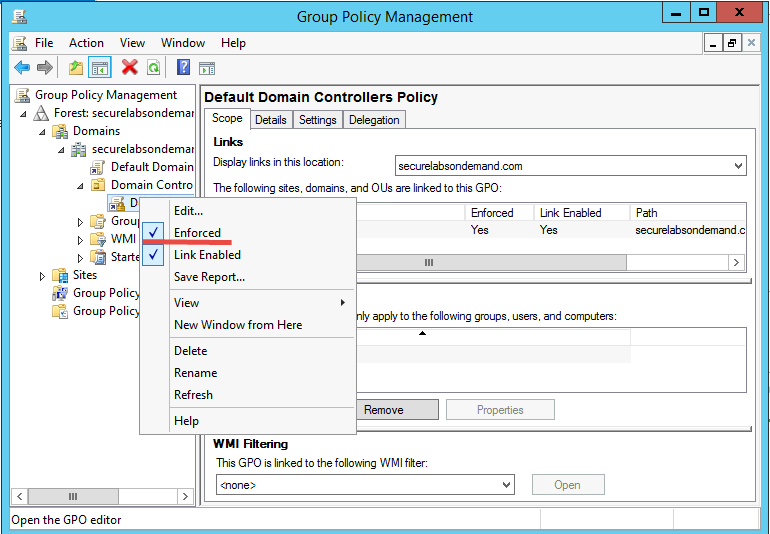
1. Password minimum length 12 character



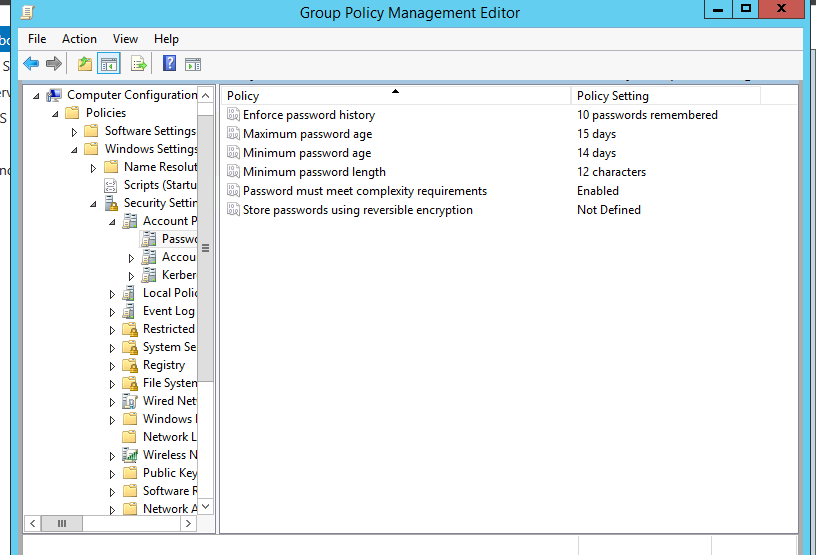
1. Enforce basic password complexity



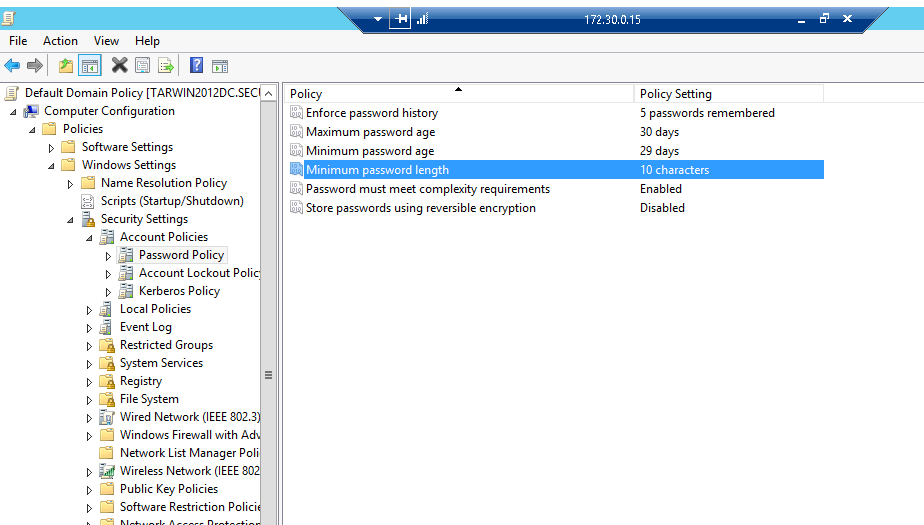
1. Domain Controller enforce



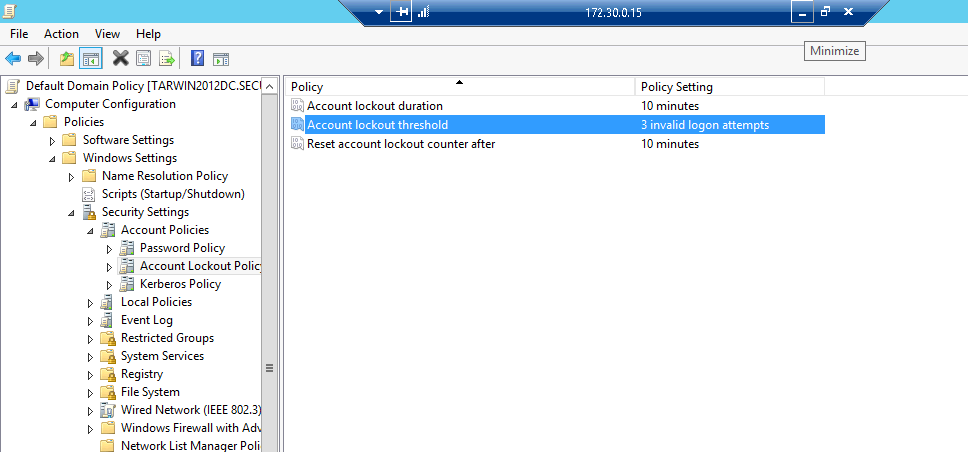
1. Summary page



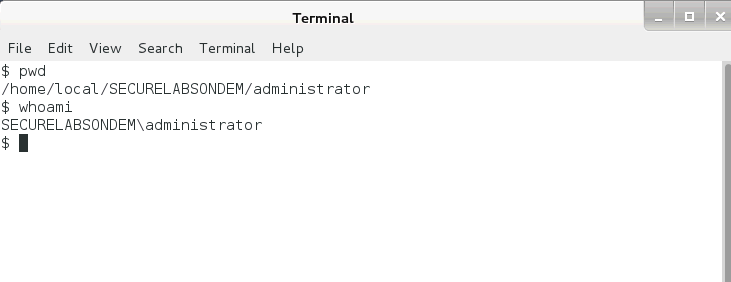
1. Report Screenshot
2. Newly configured Domain password policies



1. Configured Account Lockout Policies



1. Whoami results



1. Other additional supporting text/image content