Lab Report 3

1. Assessment Sheet
2. **What are the three fundamental elements of an effective security program for information?**

The three fundamental elements are identify, authentication and authorization.

1. **Of these three fundamental controls, which two are used by the Domain User Admin to create users and assign rights to resources?**

The two controls used by the domain user admin are confidentiality and integrity.

1. **If you can browse a file on a Windows network share, but are not able to copy it or modify it, what types of access control and permissions are probably configured?**

This indicates that the file has been set to read-only. The most possible control type is role based access control.

1. **What is the mechanism on a Windows server that lets you administer granular policies and permissions on a Windows network using role based access?**

Microsoft uses Active Directory and Group policy manager. And, Active Directory has a central database for all domain security records and it has several layers of authentication and authorization, including standard user/password and several forms of two factor authentication.

1. **What is two-factor authentication, and why is it an effective access control technique?**

Two-factor authentication means that if a user meets the two of the three conditions – something that you know, something that you are and something you possess at the same time, then we can trust the user. It’s effective because the user have to meet any two of the three conditions at the same time. If a user only has met any single condition, the authentication fails.

1. **Relate how Windows Server 2012 Active Directory and the configuration of access controls achieve C-I-A for departmental LANs, departmental folders, and data.**

In Windows Server 2012 Active Directory, it provides the system administrators with the ability to create roles, set authentication policies and build complex nested Access controls list which can maximize the confidentiality, integrity and availability because this permission settings could stop unauthorized user to access the private and value data and besides it also can prevent the internal user from modifying the data which they are not allowed to edit.

1. **Is it a good practice to include the account or username in the password? Why or why not?**

It’s not good for us to include our account or username within our password. The reason is that the more complex your password is and the more secure your account is. However, if we include the username or account in that password, it lowers the complexity of user’s password because in most cases, the username or account number is open to public or easy to get. Thus, it’s easier for an attacker to get the password through brute forcing.

1. **Can a user who is defined in Active Directory access a shared drive on a computer if the server with the shared drive is not part of the domain?**

~~If a server is not in the same domain with a user then the user could not access the shared drive of that server.~~

Yes password and username correctly and domain name also

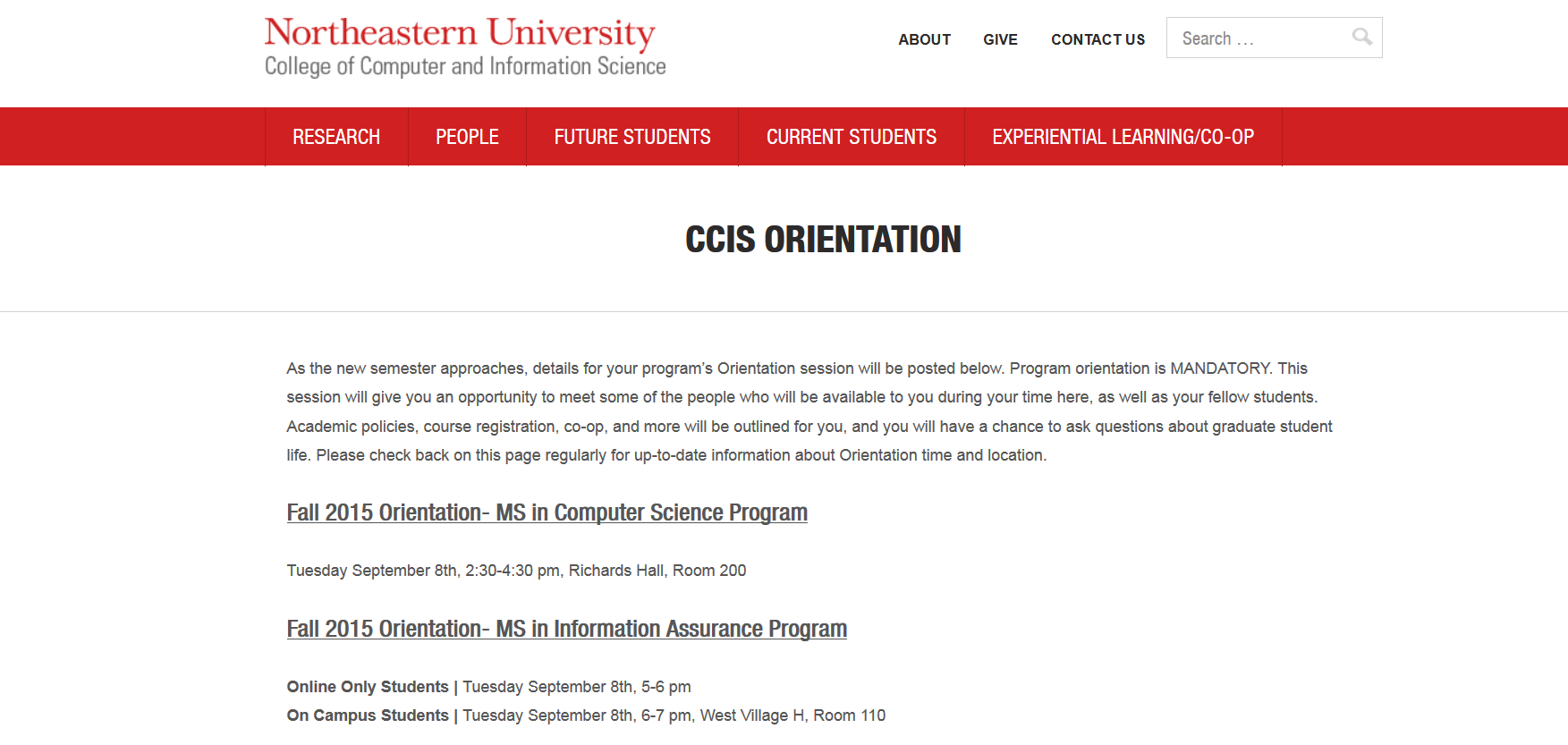
1. **When granting access to LAN systems for guests (i.e., auditors, consultants, third-party individuals, etc.), what security controls do you recommend be implemented to maximize confidentiality, integrity, and availability of production systems and data?**

We should minimize the access right to guests which means that guest only can read and write those files related and opened to them instead of giving them right to modify irrelevant files which may contains the sensitive data. In addition, we also should limit guests to use some critical equipment and access to some critical services like database. All the rights given to guest should be well and carefully designed by system administrator and security professionals.

1. Challenge Questions

**Description: Design a user access control framework for your school’s information technology department. Design a folder structure, user/group accounts, and an access control table. Use details from the lab and screen captures from your school’s website to document your work.**

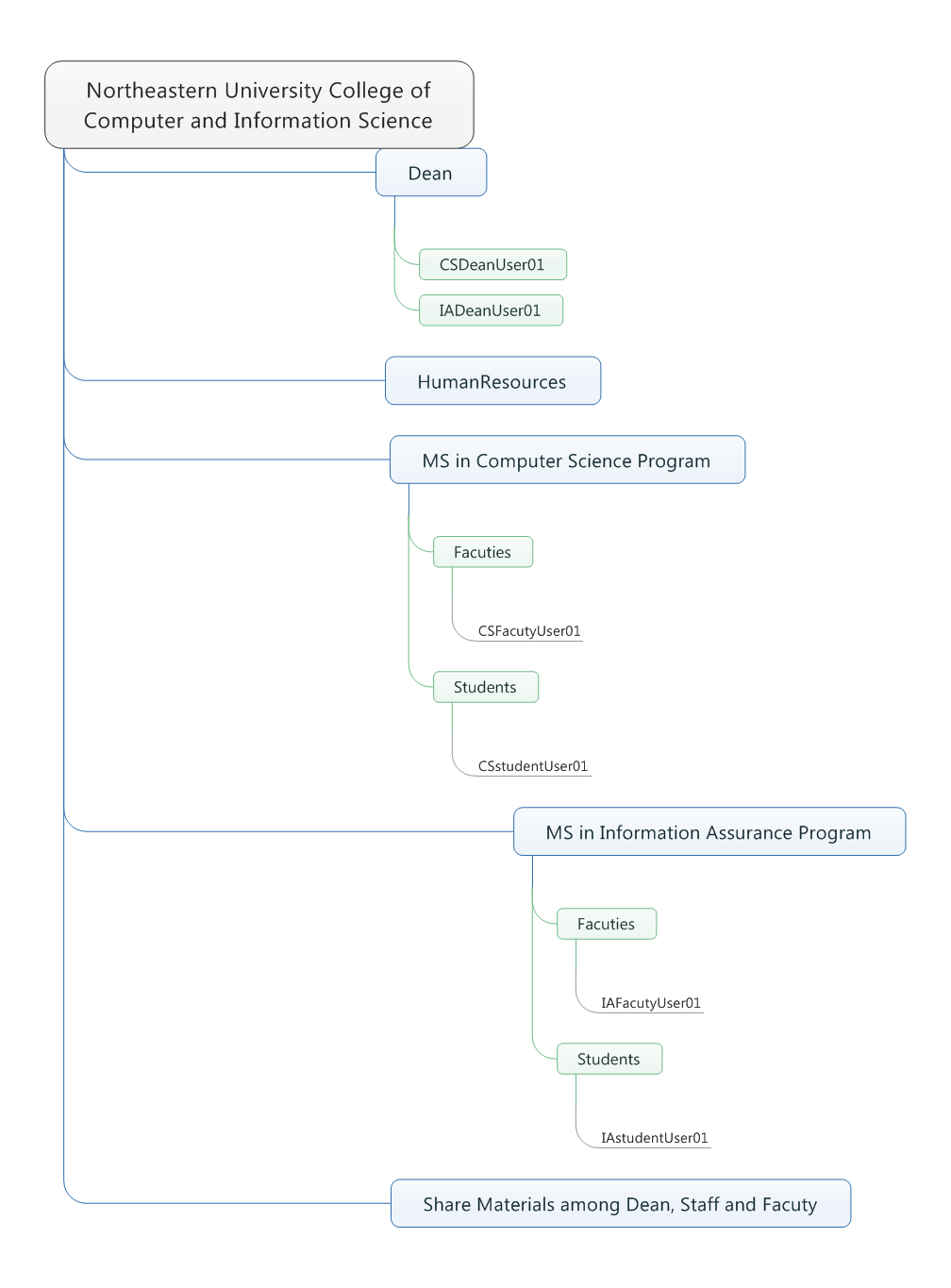
1. Northeastern University College of Computer and Information Science programs.



Explanation:

This figure I captured on our schools’ website, which shows the two graduate programs – Computer Science and Information Assurance in our college.

1. Folder structures

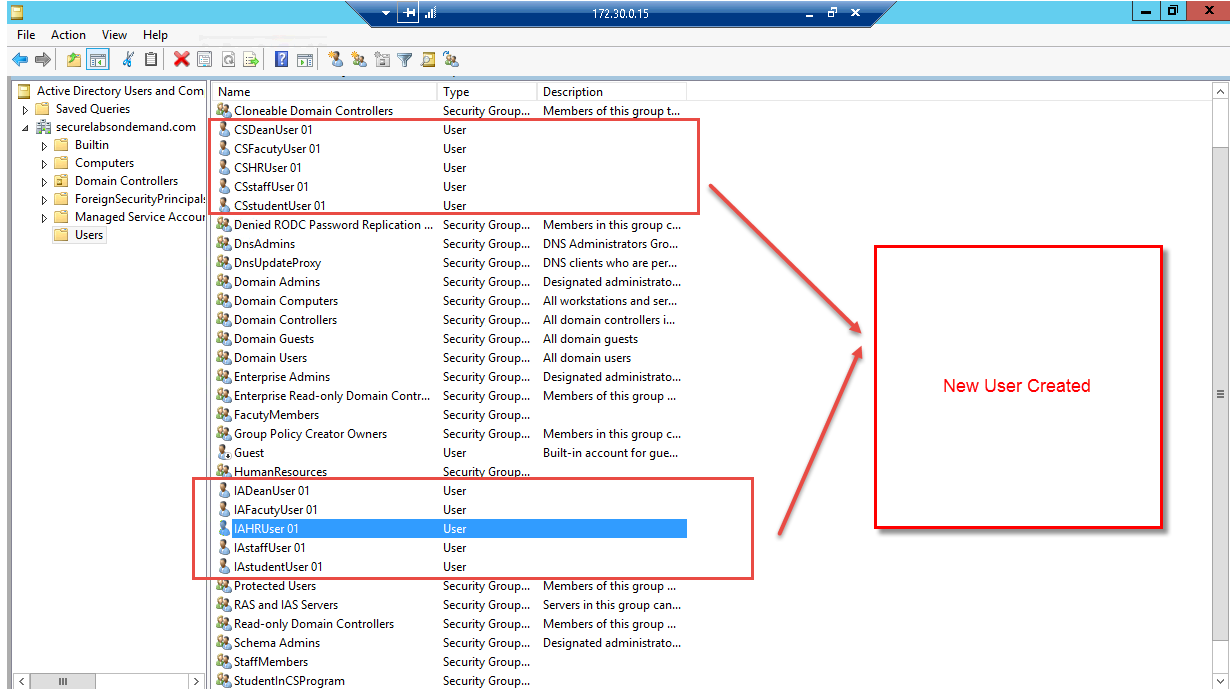


Explanation:

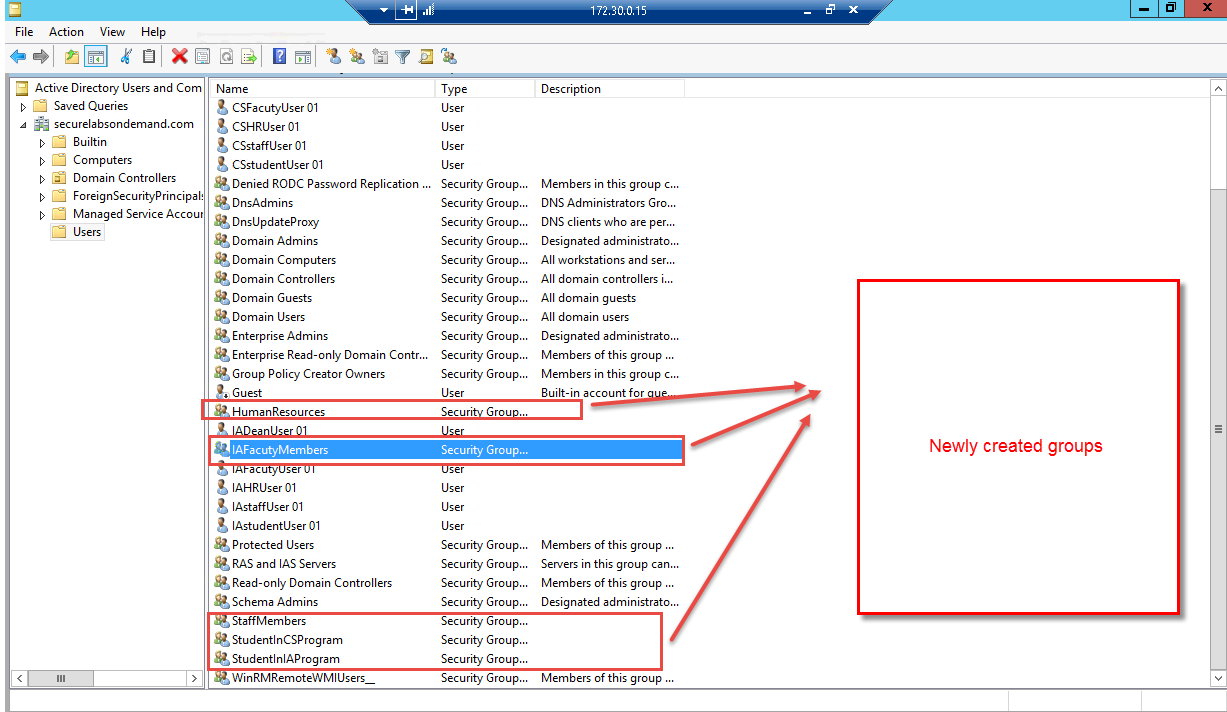
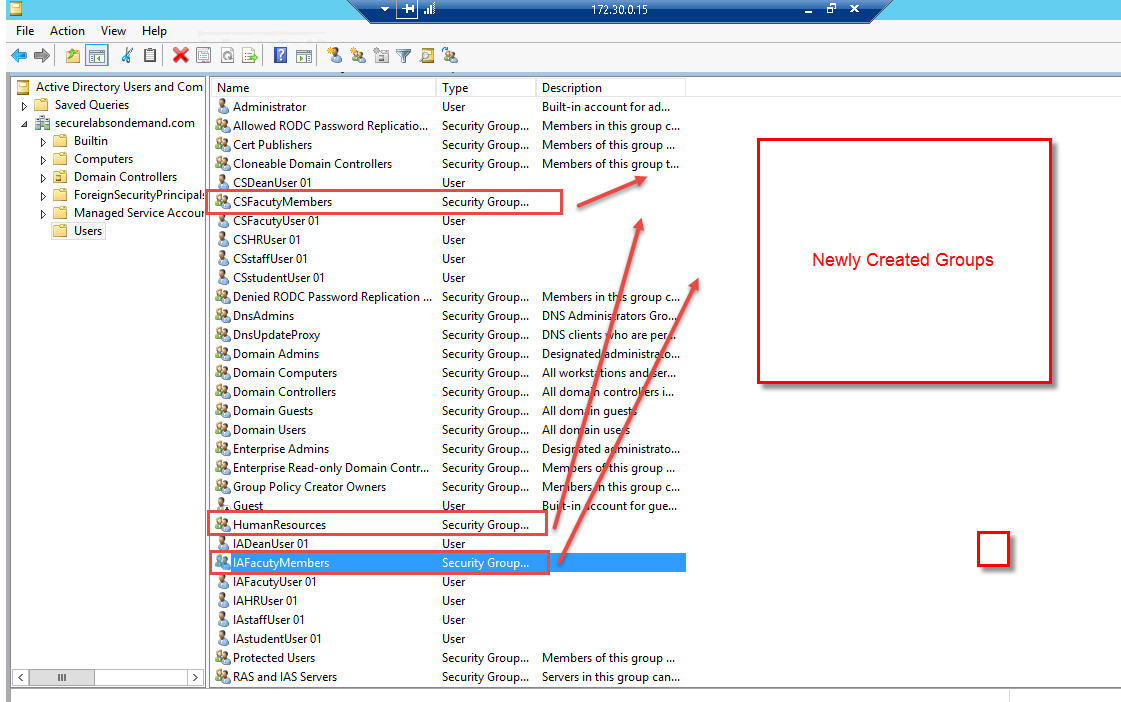
There are several rules of creating folder structures being followed as below:

1. Each degree program within this department has its own folder. In this example the two degree-folders are “MS in Computer Science program” and “MS in Information Assurance program”.
2. Each student has their own folder as their workspace. In this example the two students’ folders are “CSstudentUser01” and “IAstudentUser01”.
3. Each faculty has their own folder as workspace. In this example, the two faculties’ folders are “CSFacultyUser01” and “IAFacultyUser01”.
4. Each Dean has his own private folder. In this example, the two private folders for deans are “CSDeanUser01” and “IADeanUser01”.
5. Dean, staff members and faculty can share material in a folder. In this example, it’s “Share Material among Dean, Staff and faculty” folder.
6. Faculty and staff could visit Human Resources share folder. In this example, it’s “HumanResources” folder.
7. UserAccount/ group settings

In this question we set up 6 groups, such as HumanResources, StudentinCSProgram, StudentinIAProgram, CSFacultyMembers, IAFacultyMembers and StaffMembers, and 10 user accounts which include two deans, two faculties, two staffs, two HRs and two students for the whole college and each major has one dean, one faculty, one staff, one HR and one student.



The following pictures show that the groups that I created for this lab.



Explanation:

Due to the possible number of deans in a college, I don’t create a separate group for deans and in next part I simply add dean users separately to permission list of a folder instead of adding a dean group.

1. Access control table

In this part, due to there are too many groups in the AD, here I just list part of the access control table.

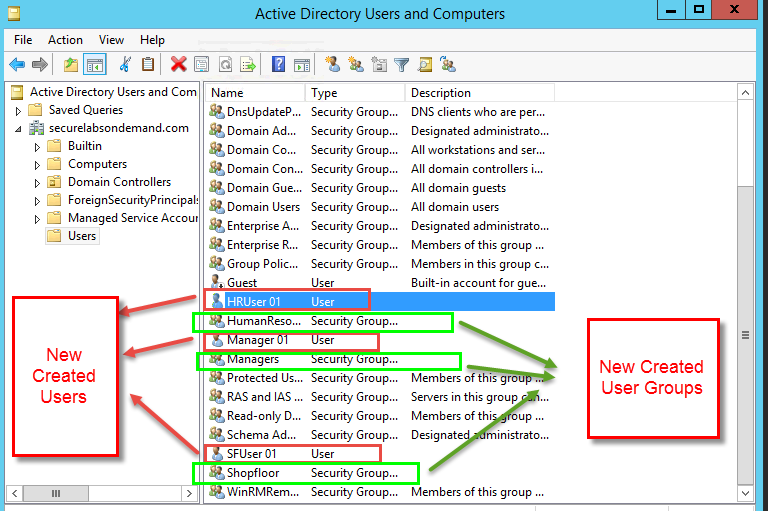
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Groups | Access to NEU CCIS folder | Access to Dean folder | Access to Human  Resource folder | Access to CS program folder | Access to IA program  folder | Access Shared Material folder(dean, staff,  faulty) |
| Human Resources | X |  | X |  |  |  |
| Dean | X | X |  |  |  | X |
| Student in IA program | X |  |  |  | X |  |
| Student in CS program | X |  |  | X |  |  |
| Staff members | X |  | X |  |  | X |
| CS Faculty | X |  | X | X |  | X |
| IA Faculty | X |  | X |  | X | X |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Users | Access to  CSDeanUser01 | Access to IADeanUser 01 | Access to  CSP Faculties | Access to CS students | Access to CSFacultyUser01 |
| CSDeanUser01 | X |  |  |  |  |
| IADeanUser01 |  | X |  |  |  |
| CSFacultyUsers |  |  | X |  |  |
| CSFacultyUser01 |  |  |  | X | X |
| IAFacultyUser 01 |  |  | X |  |  |

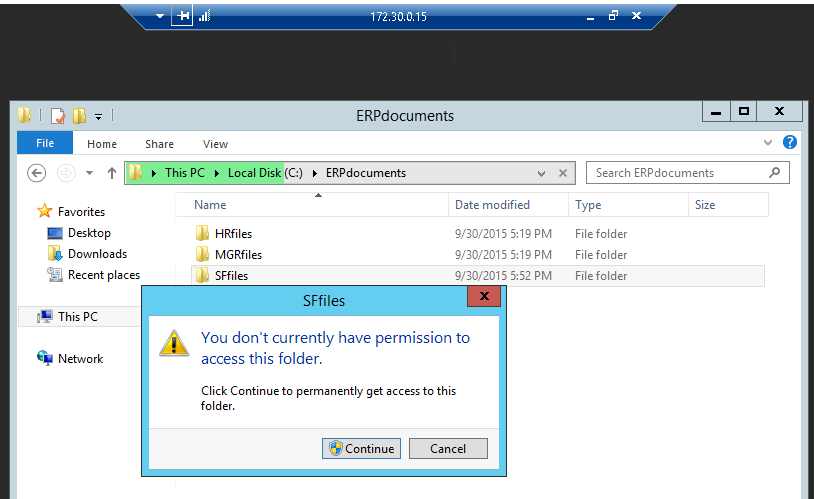
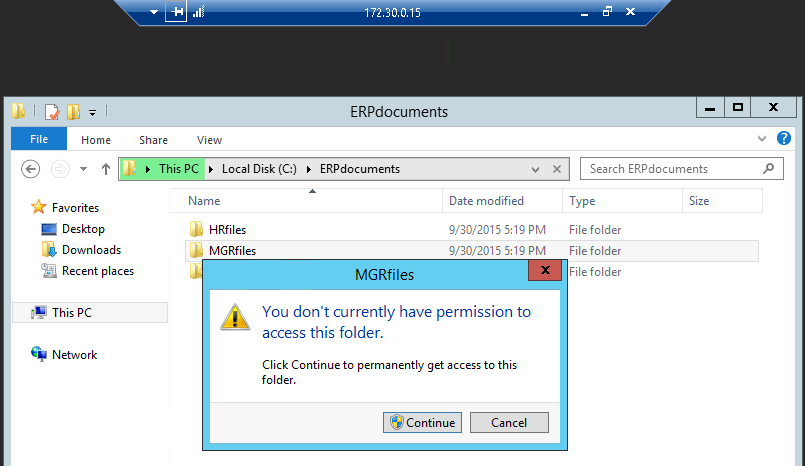
Explanation:

This table is created according to the rules that are set up in “Folder Structure” part. All the roles only can access their own folder named as their user account name expect that the faculties can see contents of students’ folder but they cannot modify any student files like add or remove.

1. Report Screenshot
2. Create new users and groups from Active Directory Management



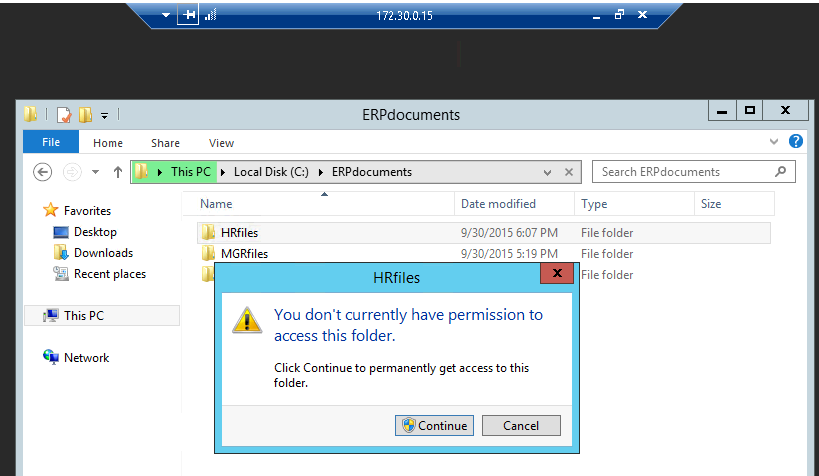
1. Unsuccessful accessing and Successful accessing
2. HRUser01 failed to access others’ folder



Explanation:

Because we break the inheritance of folder permission settings and restrict the access permission only to “HumanResources” group, so there are some access failure alerts here.

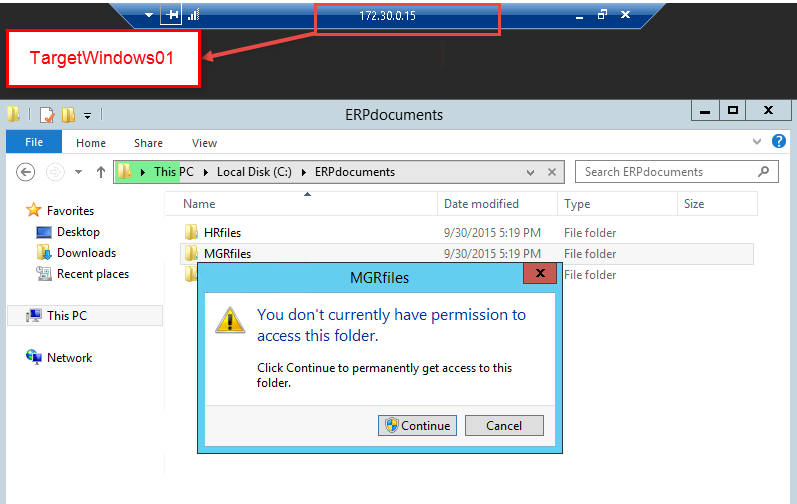
1. Manager01 failed to access others’ folder

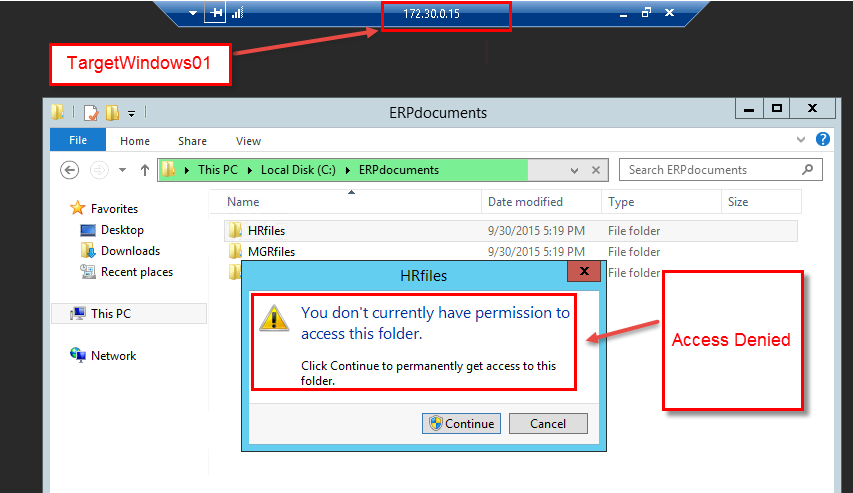


Explanation:

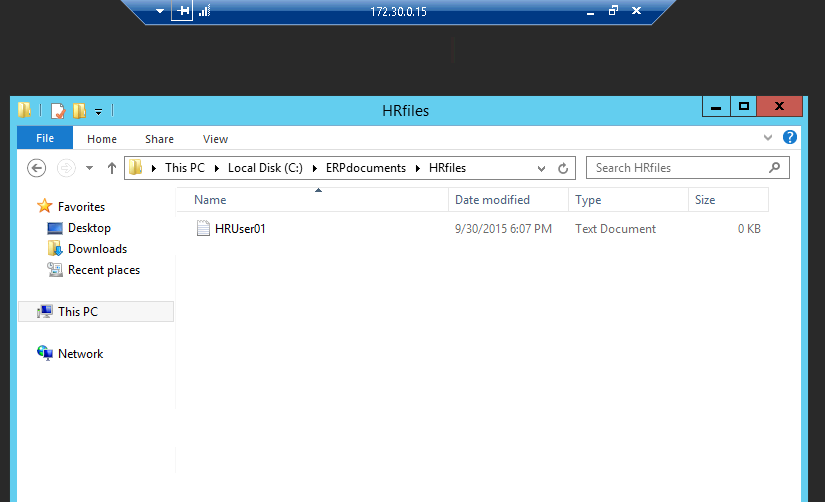
Because Manager01 has been added to both permission groups – managers and Shopfloor, so here there is only HRfiles cannot be accessed by Manager01

1. SFUser01 failed to access others’ folder

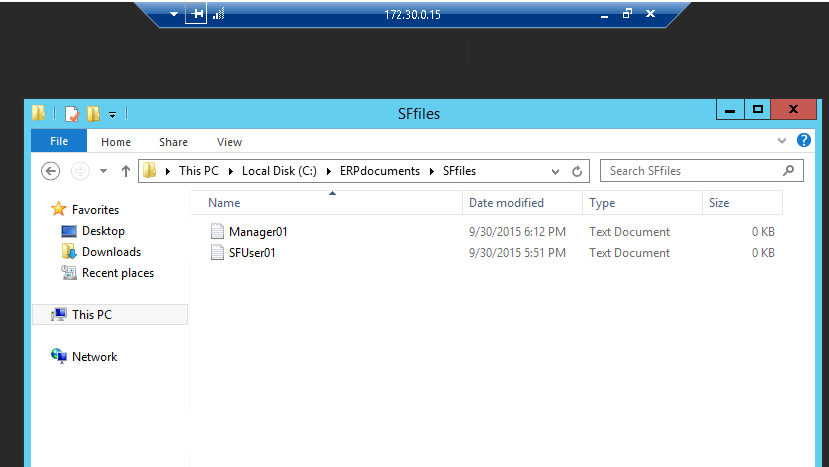
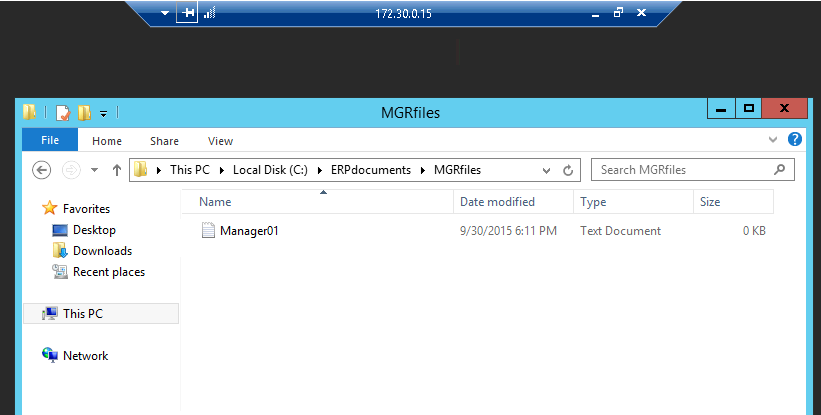




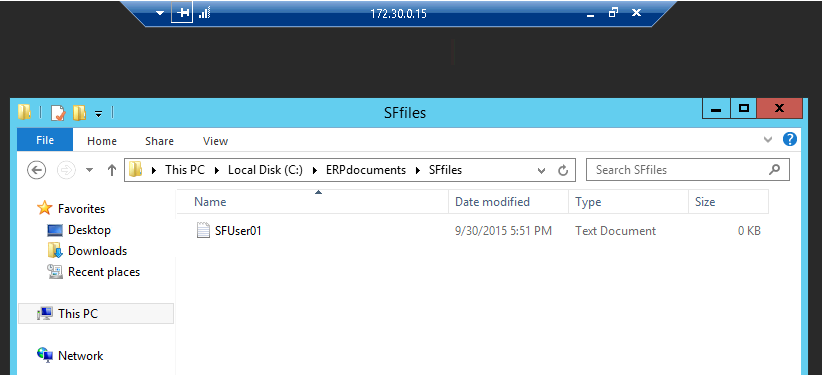
1. HRUser01 successful access its own folder



1. Manager01 successful access its own folder



1. SFUser01 successful access its own folder



1. Other additional supporting text/image content

Lab Report 4

1. Assessment Sheet
2. **Define why change control management is relevant to security operations in an organization**

In my personal idea, due to the complexity of a company’s business, the organization structures, partners, third parties are changing ever time. In addition, the technology updates in a very fast speed too. So, we cannot simple keep old controls and we need to update them in order to keep the overall system secure because old controls might not thoroughly fit the current business secure requirements.

1. **Name six policies you could enable in a Windows Domian.**

Name Resolution policy, Password must meet complexity requirements policy, ability to delete all user remote access connections policy, ability to rename LAN connections policy, prohibit access to the new connection wizard policy, ability to rename all user remote access connections policy.

1. **What is the minimum password length enforced by the Password must meet complexity requirements policy?**

Six characters

1. **What sources could you use as a source to perform the MBSA security scan?**

We can scan a computer or multiple computers by scanning an IP range.

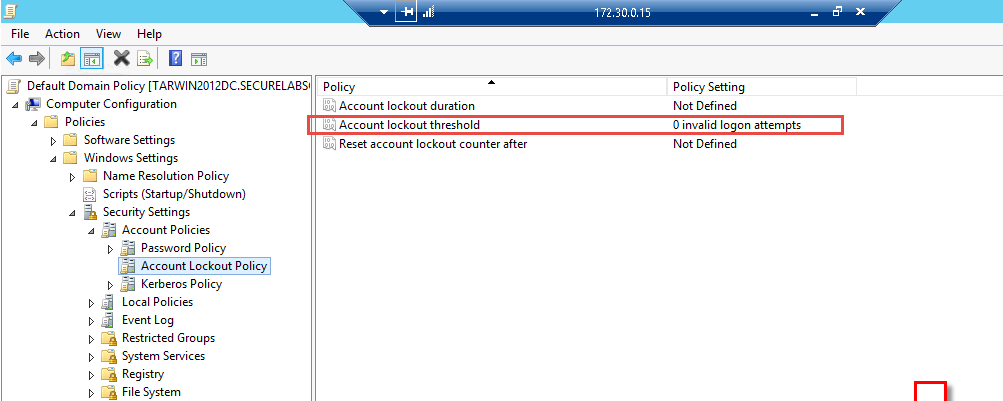
1. **What are some of the options that you can exercise when initiating the MBSA scan?**

* Check for Windows administrative vulnerabilities
* Check for weak passwords
* Check for IIS administrative vulnerabilities
* Check for SQL administrative vulnerabilities
* Check for security updates

1. Challenge Questions

**Description: Some users reported that they have occasionally experienced difficulties logging into a computer – they are being “locked out”. The CIO would like you to look at the existing Account Lockout Policy GPO security settings and modify the GPO to solve the problems.**

1. The status before modifying

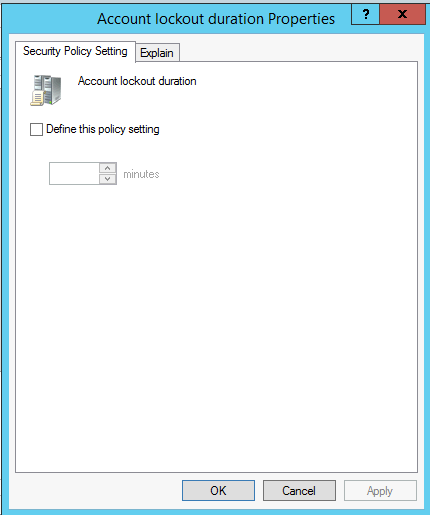
Explanation:

From the above picture we can see that yet we set account lockout threshold to 0 invalid logon attempts and other two policies haven’t been enabled.

1. Options for enhance access control within Account Lockout Policy settings

In the Account Lockout Policy settings we have three policies to help us enhance access control. Here are these three policies.

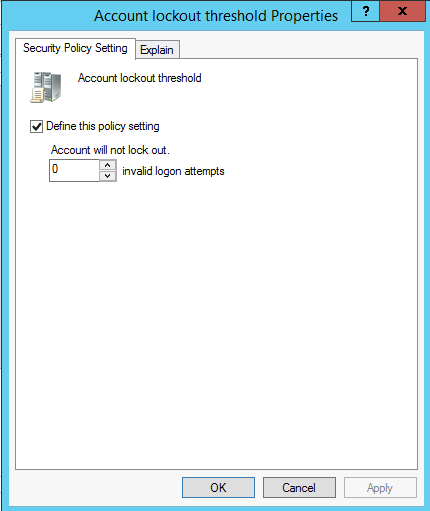
1. Account lockout duration



Explanation:

If we enabled this policy – account lockout duration, the number of minutes we set here means that after the specific time settings, the user account will automatically unlocked. If I set this value to 1 minute, that means once my logon account locked, after 1 minute my account can be available again. The maximum value of this time setting is 99,999 and the minimum value of this time setting is 0. If set to 0 that means once our accounts are locked, we only can come to administrator to unlock our accounts.

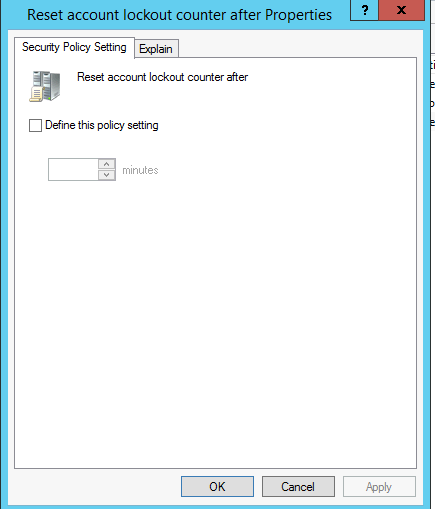
1. Account lockout threshold



Explanation:

This option specifies how many times that a user can attempt to login the server. Currently it is set to 0 that means the user account will not be locked no matter how much time he/she type wrong account/password. If we set a value above 0 like 10, it means that the user has 10 opportunities to attempt login. The maximum value that can be set here is 999.

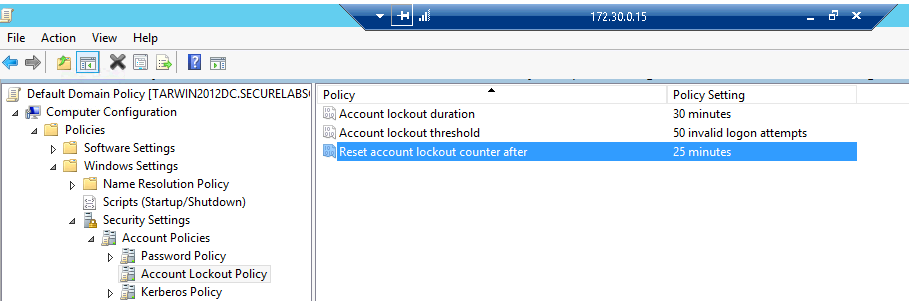
1. Reset account lockout counter after



Explanation:

This setting controls the overall time for the account lockout threshold and it always used with Account lockout out duration policy and account lockout threshold together. For example, if we set that value to 20 minutes, it means that if we used up the opportunities (specified by account lockout threshold) within the 20 minutes, after 20 minutes we can attempt as many as the value specified by account lockout threshold. The range of this value can be set from 0 to 99,999 and it must be set equal or less than the value is set by account lockout duration.

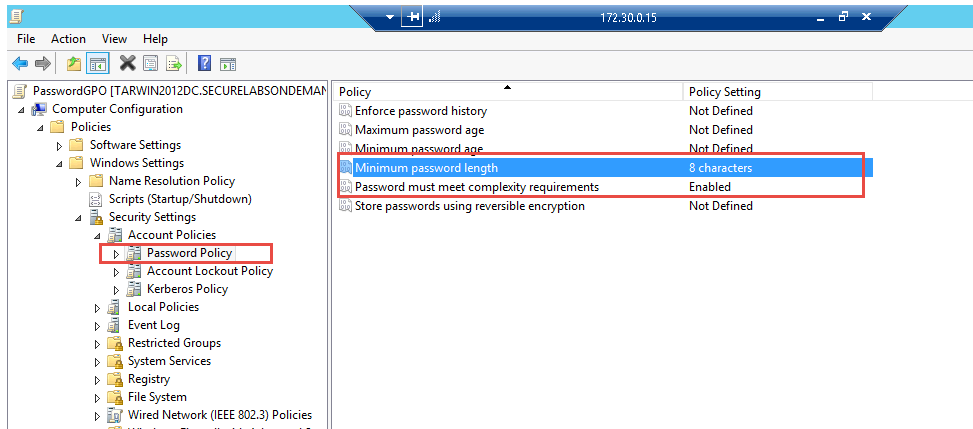
1. Modify the current policy to meet business requirement



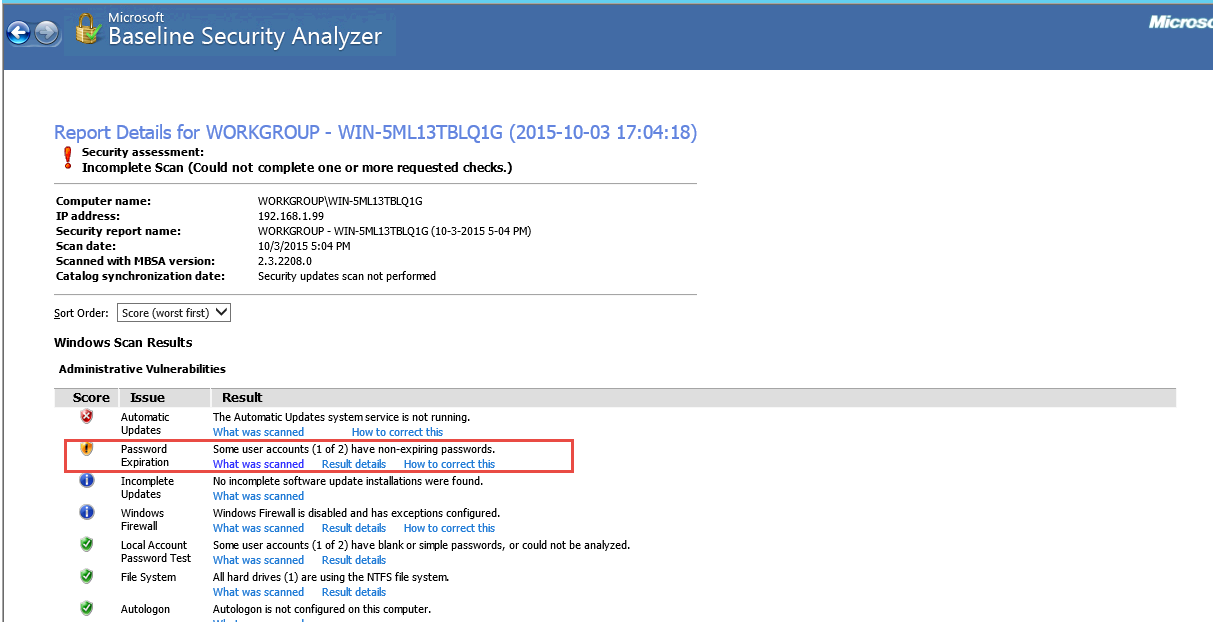
Explanation:

In this case, the lab requires us to enlarge the account lockout threshold in order to give user more chances to fail. And, also based on the security and convenience requirement we set Account lockout duration to 30mins so that the user account can automatically unlock after a certain time. Lastly, we set Reset account lockout counter after to 25 minutes and the user can get more opportunities to attempt login without waiting for too long.

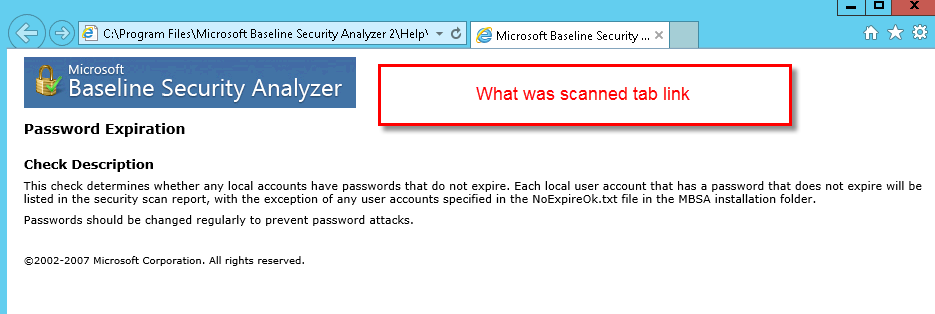
1. Report Screenshot
2. New Password GPO policy settings



1. Contents of each link from Microsoft Baseline Security Analyzer report
2. BSA Report Summary page



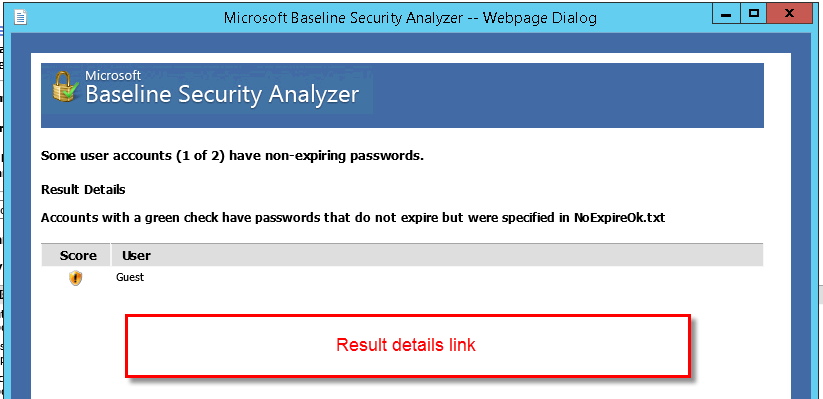
1. Password expiration - what was scanned



Explanation:

This shows that the detailed things that BSA scanned for password expiration item.

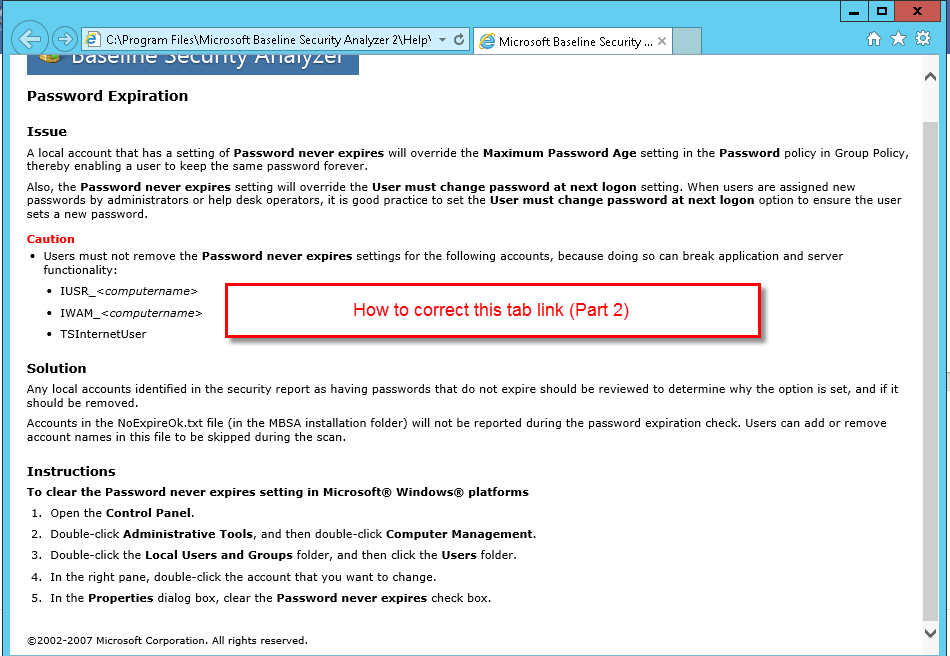
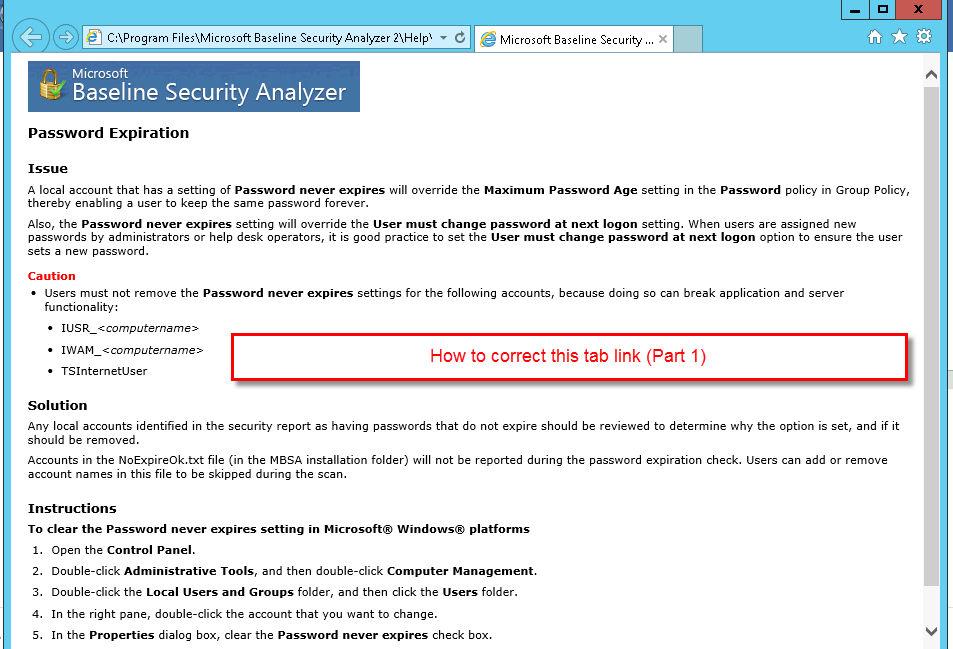
1. Password expiration - result details



Explanation:

This shows there is a never expiring password for guest account and this is dangerous for the server.

1. Password expiration - How to correct this



Explanation:

In this page, it shows several solutions to the problem identified by BSA.

1. Other additional supporting text/image content