Offensive Threats

Alaa A. Mahdi

Babylon University, College of Information Technology ,Information Network Dept.

alaamahdi@itnet.uobabylon.edu.iq

Abstracrt

This paper try to give us more details about the meaning of directory, and which type of security involved within the intended with each type of the specified directory.

The security threats pose a significant and increasing problem for organizations. This is shown by the regular stories of fraud and data loss reported daily in the media in anywhere in the world. There is a need to provide systematic protection from insider attacks because of their privileged access. Moreover, we should provide a systematic protection from the outside attacks, as well.

It is worthy to separate the duty of directory by indentifying the main two duties: the duty of the system administrator and the database administrator, and we have to recognize the difference between them. We will provide the researchers with four main threats that might be offensive to the security of directory. Moreover, we will address the nature of attack and the purpose of this attack that may encounter the directory or network assets. Finally, we will show the relation between Active Directory Security and Server Security.

Keywords: Active Directory (AD) , Directory services , Threats , STRIDE

الخلاصة

هذا البحث قد تم اعداده لتوضيح المعنى الدقيق للدايريكتوري وأمنيته واي نوع من الامنية سوف يكون مشمولاً ومقصوداً لكي يتناسب مع هذا النوع من الدايريكتوري.

ان التهديدات الامنية تؤدي الى مشكلة متزايدة ومهمة للمنظمات والمؤسسات. هذا يمكن الاستدلال عليه من خلال القصص المنتظمة عن الاحتيال والتزوير للبيانات وتقارير الفقدان للبيانات والتي يتم الاعلان عنها في اي مكان في العالم. توجد هنالك حاجة لتوفير حماية منتظمة من التهديدات الداخلية بسبب مؤهلات الوصول التي تمتلكها هذه الجهة، علاوة على توفير الحماية المنتظمة للتهديدات الخارجية.

انه لمن الجدير ان نسلط الضوء على الوظيفة الرئيسية لوحدات قواعد البيانات في النظام (دايريكتوري) من خلال تقيسم وظيفته الى قسمين رئيسيين: وهما وظيفة مدير النظام ووظيفة مدير قاعدة البيانات. سوف نقوم بتوضيح اربعة تهديدات رئيسية قد تشكل تهديد عدائي لامنية قواعد البيانات، وعلاوة على ذلك سوف نعنون طبيعة الاختراقات وهدف كل اختراق ممكن ان يهدد امنية قواعد البيانات. وأخيراً سوف نستعرض العلاقة التي تربط امنية قواعد البيانات مع امنية خادم الشبكة.

الكلمات المفتاحية: الخادم الفعال، خدمات الخادم، التهديدات، انواع التهديدات.

1. Introduction

The increasing number of breaches to the profile in which customer records, confidential information, and intellectual property are leaked has created a demand for powerful solutions that protect against the release of sensitive information. We should recognize the difference between the duty of the system administrator and the database administrator. System administrator has the responsibility to determine which user get access to the system via create an individual user account for each user (authentication) which will then be used by the operating system to determine this user. Database administrator has the responsibility to determine which user can get access to the database resources and determine which type of access control privileges will be allowed for each user (Connolly & Begg, 2009).

In any organization the directory is a collection of information related to objects. These objects often include users, computers, or contacts. Directory Services are the services which make this data available for use by others. Directory services may also be used to provide additional services to the applications and domains, such as authentication and access control (Claycomb & Shin, 2009).

Most networks provide a directory that includes both user authentication and the services of accessing control. This directory is called the active directory (AD). The active directory allows us to manage our capabilities powerfully. The directory service will include important and sensitive information about each user and related services. The process of supplying those information or services may be interfere with business operations in some situations in which there will be unregulated disclosure or disruption. Therefore, the security of directory is very important. The essential duty of the security of directory is to concentrate on the protection of information, services, and resource assets of the network as well as protect the directory information through authentication and the mechanism of access control. We must take care about how to implement the security for the information involved and the implementation of the resources that are protected by the directory service. In order to implement the security, we have to understand the active directory concept, network, and the potential threats that may encounter our resources (Melber & Kearns, 2004).

The essential process to achieve the entry and access control for all network resources is done by integrating the directory service with its operating system of the network. By the managing of both the users' rights and users' permissions, the directory service could handle the authentication of users those are attempting to get access to the network and the authorization required to allow users access resources.

2. Threats And Consequences

The directory has a fundamental role to enhance the network security in what concern to the authentication of the user. It also has the same role to enhance the network security in the operation of other applications and services provided by the network. A threat is party (program, person, or a computer) that has the ability to compromise the security of the directory or network. The security of directory is designed to protect against the following main threats that may encounter our directory or network as follows (Melber & Kearns, 2004):

2.1 Unauthorized Access to the Directory or Network

The process in which we can ensure that only the authorized users have the ability to get access to the asset of directory or network must not be underestimated. Therefore, we must spend more time and effort to protect the directory service against rouge party (program, person, or computer). The consequences of this type of threat will affect both availability and reliability and. As a consequence, it could result in loss of the revenue and the customers of organization. We must ensure that the controlling access within the use of its data will be able to recognize the coming requests to the directory service and take the right decision before these requests can affect the service (Botello, 2005).

2.2 Disclosure of Information

This threat involves any attempt controlled by unauthorized party (program, person, or computer) to expose the protected data of the directory or network. This type of threat has many forms such as the inappropriate access to the information of the file

system, access to the sensitive users account, access to the financial information, and the access to the directory information. In addition, this threat may be happened through the operation of data transmission. This type of threat will breach the confidentiality of the data especially of we use secure information (Melber & Kearns, 2004).

2.3 Unauthorized Modification of Data

Unauthorized data modification is referred to any attempt by the unauthorized user to change, delete, or corrupt to the directory information. This type of threat will attack the integrity of directory or network assets. In order to get rid of this type of threat, we should block all the holes of security which are inadvertent in our application. We have also to restrict the directory service by stipulating the access by only the authorized users to do the modification in the directory information (Melber & Kearns, 2004).

2.4 Disruption of Service

This threat represents any attempt achieved by a malicious object to prevent the intended service to serve its valid users adequately. It is called a denial of service. The means in which this attack id happened and the aim behind this attack may be changed from one to other, but it is generally involves the concerted efforts to prevent service from functioning efficiently. The common approach to do this attack is by saturating the attacked network with external communications requests, so that the rendered effectively will be unavailable. The denial of service is implementing by either forcing the attacked network to reset or consuming its resources (Melber & Kearns, 2004).

3. Addressing The Threats

In order to address the threat that intimidates the security of directory service and sensitive information, we have to understand the nature of the attack and the purpose of this attack that may encounter the directory or network assets. We will use the STRIDE acronym to address the expected threat that may encounter the directory or network assets as follows (Melber & Kearns, 2004):

3.1 Spoofing

With spoofing, the attacker tries to pretend as to be someone or some process which has a valid access to the directory. The attacker may use the username and password of another legal user or service which has the permission to access the directory. In order to protect our system from this type of attack, we have to consider the policies necessary to ensure the security of both user name and password information for all users accounts which have access to the directory (Melber & Kearns, 2004).

3.2 Tampering

This type of attack will be conducted either directly by the unauthorized person or indirectly by using software which is designed to modify or corrupt the information of directory. This attack involves any attempt that is tried to tamper with the asset of directory by unauthorized person or software. In order to get rid of this type of attack, we should keep our security patches up to date to block all the holes of security which are inadvertent in our application. We have also to restrict the directory service by stipulating the access by only the authorized users to do the modification in the directory information (Melber & Kearns, 2004).

3.3 Repudiation

With this type of attack, the administrator does not have the ability to recognize the identity of attacker who achieved the unauthorized operation(s) with the system. If any change to the directory information is not being audited, then it will not be able to trace back to the source of the unauthorized changes that is happened to the log information. In order to get rid of this type of attack, we should perform both the stringent authentication and the auditing of the directory (Melber & Kearns, 2004).

3.4 Information Disclosure

It involves the exposing of the protected data by unauthorized party which has access to the asset. This type of threat has many forms such as the inappropriate access to the file system's information, the illegal party which has access to the sensitive users account, access to the financial information, and the access to the directory information. This threat may be happened through the data transmission the network. In this case, the information will be captured through the use of application which has the capabilities of similar packet monitors. This type of threat will breach the confidentiality of the data especially of we use secure information. One approach to overcome this threat is by using a prior packets encryption mechanism before transmitting data. In order to defend the threat of information disclosure, we should control the access to the sensitive objects of directory, file systems, and the necessary baseline information. The types of attack that use a convincing authentication will still has the ability to disclose the information and the technological mechanism cannot prevent this type of attack. In order to increase the awareness of the security, we should provide a security training tutorials and courses to the people whose have access to the sensitive information and directory to restrict the successful of disclosure threats (Melber & Kearns, 2004).

3.5 Denial Of Service (Dos)

It is stands for denial of service. DoS attack may be simple to result in only shutdown the victim's server remotely, or it may be complex that will lead to expose the victim's system by saturating it with external communications requests. In both cases, the network service cannot respond to its valid users, or it responds slowly. This threat represents any attempt achieved by a malicious object to prevent the intended service to serve its valid users adequately. In order to get rid of this type of attack, we should monitor the performance and enhance the capabilities of automated alerts (Melber & Kearns, 2004).

3.6 Elevation Of Privilege

With this type of attack, the attacker whether s/he is authorized or unauthorized person has the ability to tamper and change the permission access (privilege) in the user accounts to control over directory, the setting of file system, and network. This attack will enable the attacker to disable the function of auditing, monitoring, and any other tracking mechanisms. In order to get rid of this type of attack, it is preferable to use both intrusion detection system and intrusion prevention system to enhance the capability of the security team of detect this type of attack (Melber & Kearns, 2004).

4. The Relation Between Active Directory Security and Server Security

These two issues are interrelated because Active Directory administrators dictate who is in a group, and permissions to server resources are usually assigned at the group level. If Active Directory roles aren't regulated, unauthorized users might be added to a

group and thereby gain access to resources for which they don't have clearance (Viejo, 2013).

5. Database Users and Privileges

IT departments are under consistent pressure to reduce cost, enhance security, and improve compliance to support ever-competitive business. Databases are critical components of enterprise IT infrastructure, so it is a key to centralize and integrate database users and privileges into an enterprise identity management framework (ORACLE, 2015).

We prepared a table to show examples for those frameworks and their benefits as mentioned below:

Framework Name	Benefit
Enterprise User Security (EUS), an Oracle Database Enterprise Edition feature.	Leverages the Directory Services and gives you the ability to centrally manage database users and role memberships in an dedicated directory. EUS reduces administration costs and increases security.
IBM Security Directory Suite.	Provides a trusted identity data infrastructure for authentication. It includes Directory Server, Federated Directory Server, and System for Cross-Domain Identity Management (SCIM). IBM Security Directory Suite comes in a virtual appliance format.
User Directory Software Blade.	• Activate centralized user management on any Check Point Security Management server. • Centralized user management throughout the enterprise. • Eliminates risks associated with manually maintaining and synchronizing redundant data. • View, modify and create users, groups via easy-to-use Smart Dashboard GUI.
Microsoft Active Directory integration.	• Ensures secure access to your security software and physical facilities is up to date. • Promotes cooperation, sharing of data, and consistency throughout your organization. • Streamlines user management, taking human error out of the equation. • Simplifies cardholder management, allowing your team to be more productive. • Automated synchronization eliminates burdensome paperwork and emails for managing employee access. • Security groups are visible within Security Center leading to quick selection of groups and users to sync.
Windows Security and Directory Services for UNIX using Centrify Direct	• Specify which Active Directory users and groups can log on to a specific UNIX computer or group of

Control.	computers. • Control user access to UNIX computers across the entire Active Directory forest, regardless of the organizational structure you use or where users are defined in that structure. • Map local UNIX accounts, such as the root user, to Active Directory accounts for centralized control over access and passwords. • Identify specific local UNIX accounts to be authenticated locally rather than through Active Directory. • Migrate multiple existing UNIX account information stores into Active Directory, as needed. • Enable authenticated users to connect to Web applications without being prompted to log on again with their Active Directory credentials (single sign-on). • Take advantage of Microsoft's Group Policy to apply settings and controls for UNIX users and computers.

6. Conclusion

A collection of information related to objects in any organization is called as a directory, and it has various services. These services make this data available for use by others. Directory services could be used to provide additional services to applications and domains, as well. It is very important to separate the duty of directory by indentifying the main two duties. We recognized the difference between the duty of the system administrator and the database administrator. Later, we presented four main threats and their consequences that might attack our directory or network. We used STRIDE acronym to address six types of attack to understand the nature of the attack and the purpose of this attack that may encounter the directory or network assets. We identified the interrelation between the active directory security and server security. Finally, we illustrated with a table for some known enterprises and their benefits to ensure the role of databases which is a critical component of enterprise IT infrastructure.

References

Botello, B. (2005). *Directory Services: Critical to Effective Identity Management.* USA: Sun Microsystems, Inc.

Claycomb, W. R., & Shin, D. (2009). Threat Modeling for Virtual Directory Services. *IEEE* , 149-154.

Connolly, T., & Begg, C. (2009). *Database Systems A PRACTICAL APPROACH TO DESIGN IMPLEMENTATION, AND MANAGEMENT.* Glasgow: Pearson Education International.

Melber, d., & Kearns, D. (2004). *The Administrator Shortcut Guide to Active Directory Security.* USA: www.realtimepublishers.com.

ORACLE. (2015, February). ORACLE DIRECTORY SERVICES INTEGRATION WITH DB ENTERPRISE USER SECURITY. Retrieved January 12, 2016, from

www.oracle.com: https://www.google.iq/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwj0su6KqqPLAhUIMJoKHev4AGoQFggbMAA&url=http%3A%2F%2Fwww.oracle.com%2Ftechnetwork%2Fdatabase%2Fsecurity%2Fdirsrv-eus-integration-133371.pdf&usg=AFQjCNHiBk0VWMBbtvev6VNkhF1eHtHhWQ&sig2.

Viejo, A. (2013). *Active Administrator & Security Explorer - Dell Software.* Retrieved November 30, 2015, from www.dell.com: https://www.google.iq/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwjt_J39qKPLAhVGYJoKHYOTDYcQFggbMAA&url=http%3A%2F%2Fsoftware.dell.com%2Fdocuments%2Factive-administration-and-security-explorer-datasheet-19386.pdf&usg=AFQjCNHHTligbCAh-ZgLt1qKQU1_-Z.