Active Directory and Related Aspects of Security

Afnan Binduf, Hanan Othman Alamoudi, Hanan Balahmar, Shatha Alshamrani, Haifa Al-Omar, Naya Nagy
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY
Dammam, Saudi Arabia
fbinduf@hotmail.com, hananamoudi2@hotmail.com, hanan50@outlook.com, shtha.7.homoud@gmail.com, Haifaomar.ho@gmail.com, nmnagy@iau.edu.sa

Abstract

This paper discusses active directory that is used across many organizations to centralize control of users' logins to organization resources and network. A Saudi company that does not implement active directory which enables centralized, secure management of an entire network is analyzed in this paper. Active directory servers have some vulnerabilities that affect the security of active directory. There are many guidelines recommended to address security issues. Active directory has built-in support of security controls, and there are many possible ways to enhance the security of active directory and the network. Not implementing active directory in large organizations lead to the loss of control over user's resources and information which might result in serious security threats.

Keywords: Active directory, Group Policy Preferences (GPP), Kerberos protocol, Domain controller, IPSec protocol, change auditor, failover cluster instances, Domain admin, AlwaysOn availability group, Azure active directory

I. INTRODUCTION

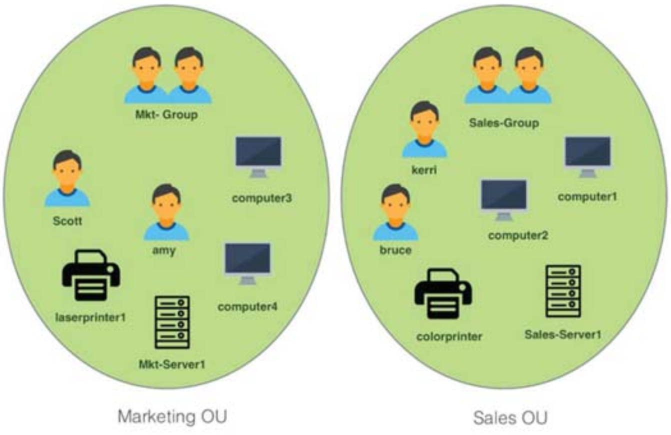
Nowadays most of the companies use active directory, and it is hard for any company to work without the active directory. Active directory is a central repository for information of all company's resources that exist in the network, like employees, groups, devices, printers, programs, and documents. So, the administrators of the Active directory can efficiently manage the company's information from a central repository. [1] Although most of the companies use active directory, however, only a few of the companies know how to use it securely and know how to avoid vulnerabilities in active directory. Information system auditing has been done on a Saudi company. The communication was with a manager in the company to perform this audit. The audit that has been done focused on important risks that affect the security of the company. This company uses the different system similar to active directory to manage financial department only. This is considered one of the risks that threaten the security of the organization. Active directory comes with windows server and it can be used to manage entire company. It designed to work with window operating system. It provides scalability, security, and central management. The company requested to remain anonymous for security reasons. This company is producing indoor and outdoor lighting products. The result of this audit recommended that active directory should be implemented in all department of the company, so the main goal of this research based on IS auditing experience with this company is to discuss the important role of active directory in managing users and resources of the organization and maintaining acceptable levels of security in the system. In this paper, vulnerabilities of active directory servers are discussed in section 2. The third section discussed the security of active directory which is the alert feature, maintain integrity and confidentiality in active directory network, user authentication in active directory and active directory availability group. At the end of the paper, future work and conclusions are described.

II. BACKGROUND

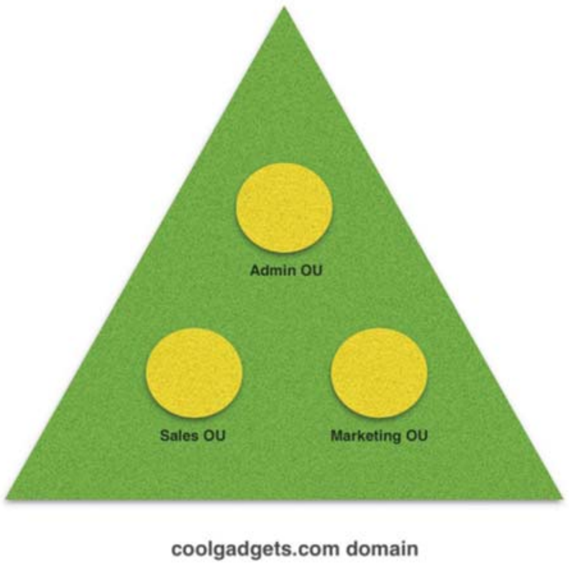
The active directory provides central services because it contains all contents of organization database such as resources, service, user accounts, shared folders, etc. To manage network resources. Active directory domain service is a service provided by Windows, started in Windows Server 2000 and evolved over the years through the versions of Windows and has reached Window Server 2012. It allows the admin to set a policy, add a user, and control authentication. [2] There are two parts of the active directory structure: the first part is a physical structure which consists of location and servers configured as domain controllers and the second part is a logical structure which consists of four organizing components that are considered as a container, based on the geographical area shown on figure 1. An organizational unit (OU) represents a city, the domain represents the state, a tree represents the country, and a forest represents the continent. Since the company's scope ensures several elements that need to be grouped together, it means all the information present in the central location that facilitates the work process in the organization. [3]. If the active directory is not implemented by the organization, it will lose the following advantages:

- Simplifies network resource management and security policy management in a hierarchical organization of active directory. [3]
- The ability to meet the increased and growing needs of the organization. Therefore, after the active directory installed it allows modifying the properties and adding objects. [3]
- Allow managing the organization from one point. [3]
- It enhanced security by providing a secure login more than another directory service. It's used IPSec protocol in Windows Server 2000/2003 [4] and Kerberos protocol used in Windows Server 2012. [1]

The following papers [5], [6] discuss another aspect related to active directory which are different from the topics discussed in this paper. The first article discusses continuous auditing tool of Active Directory. The second paper design method that are used to improve the confidentiality of active directory service.



I Active Directory organisation unit



II An Active Directory domain and OUs

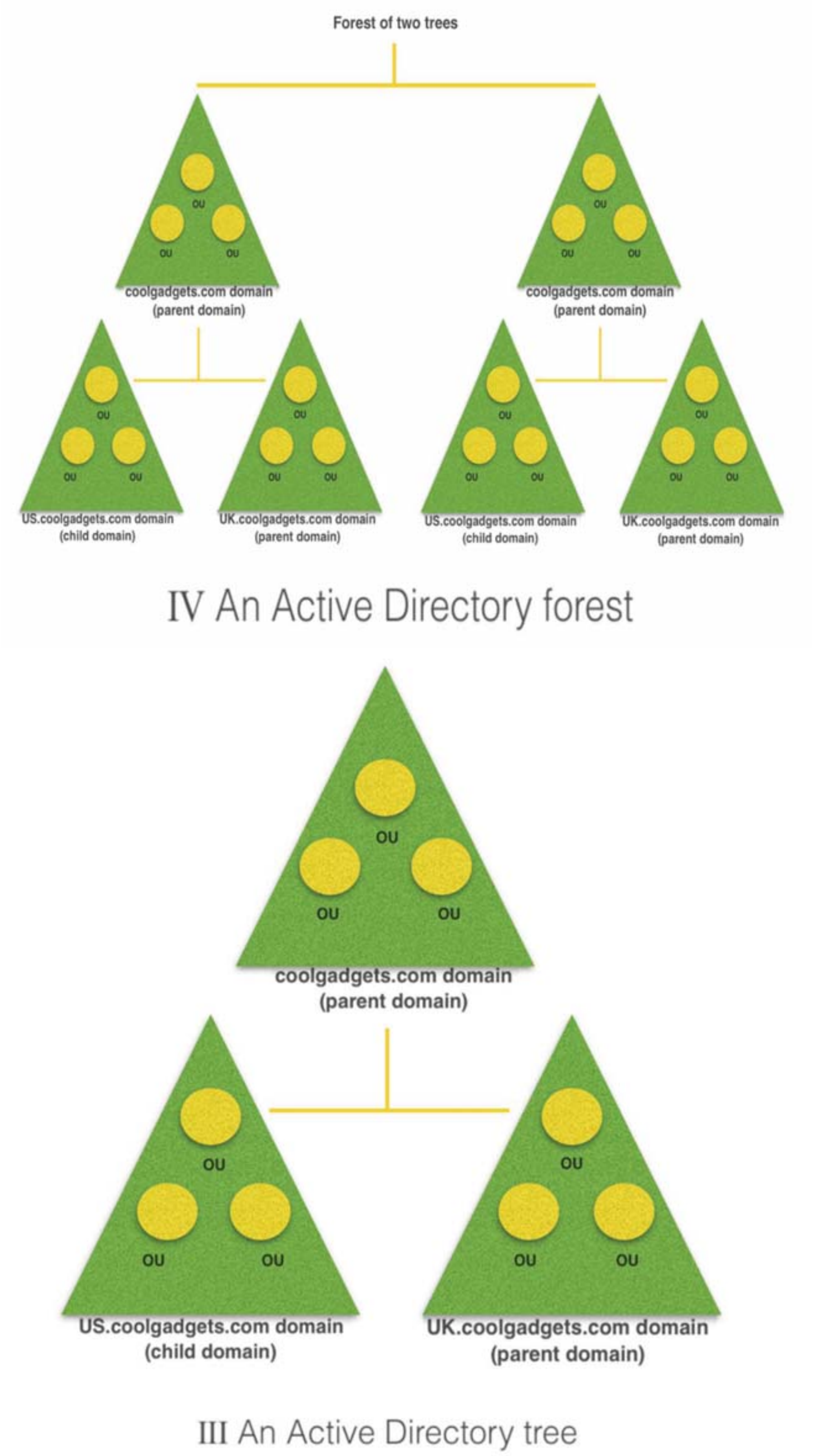


figure 1: Types of active directory logical structure

III. Vulnerabilities of Active Directory Servers

The Saudi organization under scrutiny does not use an active directory to control the employee's access resources, so the organization should choose an appropriate type of active directory server because many of these servers have a vulnerability that Microsoft organization still make security updates to resolve the vulnerabilities. Windows Server 2000 and 2003 has a vulnerability like remote code execution and prone to denial of service attack(DoS). Remote code execution it happens when the attacker executes some arbitrary code on the system to allow the attacker to control the system by creating the account, changing, deleting data. Denial of service attack happens when the attacker sends malicious queries to a system. The attacker can exploit the vulnerability and make the Active Directory service become unresponsive [7]. Denial of service does not stop here it also attacks Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2 [8].

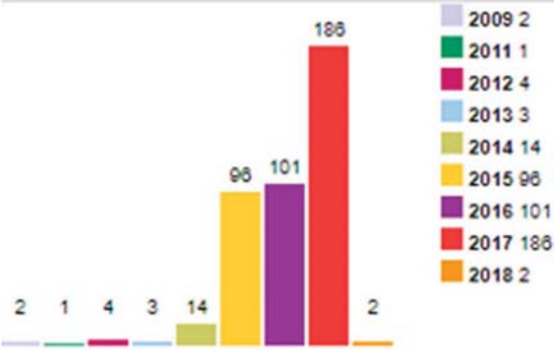


figure 2: analysis of vulnerabilities by year that mentioned in https://www.cvedetails.com/version/121761/Microsoft-Windows-Server-2008-.html.

Figure 2 shows that exploit vulnerabilities increase over time, as applied to the year 2017. From figure 3 and 4, the number of vulnerabilities is 186 and the most common type of vulnerability in windows server 2008 is gain information and gain privileges in windows server 2012.

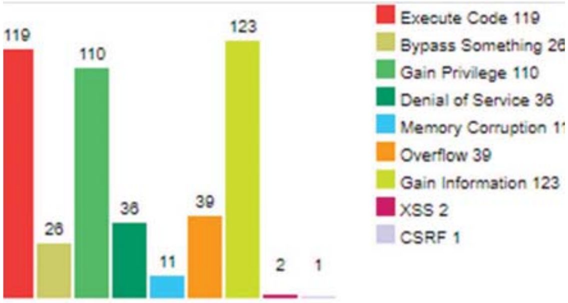


figure 3: analysis of vulnerabilities by type that mentioned in https://www.cvedetails.com/version/121761/Microsoft-Windows-Server-2008-.html

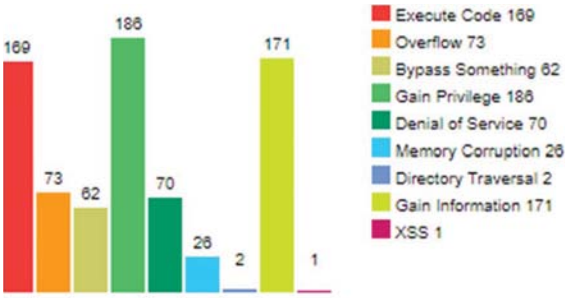


figure 4: analysis of vulnerabilities by type that mentioned in https://www.cvedetails.com/product/23546/Microsoft-Windows-Server-2012.html?vendor_id=26.

From the figure 3, it shows the other vulnerabilities that affect active directory like Cross-site scripting (XSS) vulnerability in Active Directory Certificate Services. Cross-site scripting exists on Microsoft Windows Server 2003 SP2 and Server 2008 Gold, SP2, R2, and R2 SP1.Cross-site scripting happens when the attacker injects a web script code. The attacker can exploit this vulnerability by sending to the client/user a link and make them visit the vulnerable website by clicking on the link [9]. Second vulnerability that affects Microsoft Active Directory is a buffer overflow. Exploits this vulnerability can allow attackers to execute arbitrary code with network service privileges. When the attacker fails to exploit the Cross-site scripting vulnerability it will cause a denial of service and it can happen in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 [10].

IV. Security Issues of Active Directory

There are a lot of security issues that give the attackers opportunities to gain access to the Active Directory. Here are the most common active directory security issues.

- Service Accounts has over-permissioned.

A service account is an exceptional type of account that often provide a lot of privileges and permit services to contact with the underlying operating system. Further privileges added to this Account can be used maliciously to heighten of access rights which are a serious security danger. It is very important to make sure that each Service Account is deputize required right. The service that running underneath service account has a credential in LSASS (protected memory) which can be extracted by an attacker. If the stolen credential has admin rights, the domain could be compromised [11].

- A lot of Domain Admins.

The entire administrative rights of " all workstations, servers, Domain Controllers, Active Directory, Group Policy" are done by the members of Domain Admins. By default, this is too excessive power for any account in a company. Typically, Domain Admins involve Service Accounts and further groups that are not immediately linked to Active Directory administration. Preferably the Domain Admin group should be idle to make sure that each role has only the required right to execute tasks associated with that role. Only Active Directory administrators require privileges Domain. Anyone is not handling Active Directory in an active way, must not be in Domain Admins anymore [11].

- The same passwords for a local Administrator account on all systems.

Most system administrators using the same username and password for local administrator account, this allow administrator to log on to other accounts using the same username and password, which is not good idea from a security point of view, because this makes it easy for the attacker to gain access to all systems once the attacker get the credentials of one local administrator account, so it prefer to have a unique credentials for each local administrator account [11].

- Domain Controllers are running an old version of OS.

Further advance of security improvements appears with every consecutive version of Windows Server, and prior security defect is patched. If the newer release of the operating system is not installed, some security dangers will appear. For instances, Domain Controllers faced security risks when it is running in the older version of Windows Server. [11]

- Using Group Policy Preferences (GPP) to handling credentials.

More functionality is providing to the system administrators by Group Policy Preferences (GPP). Group Policy Preferences (GPP)can change the password of the local administrator account, create local account and services, etc. the password that stored in the XML file which placed in SYSVOL share is created significant issues because any domain can gain access to the files in SYSVOL. If the credential is previously configured in GPP, eliminate it directly and Remove the files [11].

- The password length of Service Accounts is less than 20 characters.

It is simple to request data that has been encrypted with the password of Service Account. It is feasible to decode the data by using brute forced offline and reveal the password for the account if the password is supported by the Kerberos network authentication protocol. This issue can be mitigated when the password of Service Accounts is more than twenty characters [11]

V. The Security of Active Directory

A-Alert Feature

Most companies want to know exactly who did a specific action in their workplace? The main issue is that they need to be informed by some alert method when someone changes such a file, and this can happen using Active Directory Auditing Agents. Knowing every single event in the system increases the level of accountability. Auditing, protection, and alert are advantages provided by Active Directory Change Auditor to enhance the accountability. When an event occurs, people who have the right will be alerted automatically. One more example that admins set the configuration for tracking the use of the account. If you install a new service in the organization, usually the service will be available for pre-selected devices. With change auditor service alert, can be configured to maintain the accounts used with other nodes and admins can be notified [12].

B-Maintain Integrity & Confidentiality in Active Directory Network

As active directory database contains the most sensitive data focusing on the secure active directory and its network traffic is important. IPsec which stand for IP security is network layer protocol that secures the traffic on the network and protects from different network attacks. IPsec used to add a security layer to the network and therefore participate in protecting the active directory. IPsec can secure the transmission between two ends by encrypting packets or by securing transmission path between two IP addresses. The encryption provided by IPsec protect against eavesdropping attack that might affect the confidentiality through the network and cause further attacks. IPSec provides a checksum to ensure that packet did not alter or modified through its transmission and to detect attacks such as session hijacking and man in the middle. Domain controllers host active directory database and because of that protecting domain controllers is necessary. Domain controller must be placed in a secure physical place to protect it from unauthorized access and modification of the files or configurations. Setting a strong password to administrative account is also an important step because this account has access to the whole network. Renaming or disabling administrator account may provide more security since it is targeted by hackers. Installing security updates is necessary to patch vulnerabilities that might be exploited against the system. Antiviruses play important role to protect domain controllers from malicious malware and should be up to date to detect new viruses and malware [4].

C-User Authentication in Active Directory

Users access to network resources are controlled through logon process where the user must provide his or her credential to gain access to services and applications [13]. User authentication mechanism in active directory carried by Kerberos protocol. Kerberos protocol is security protocol that provides flexible authentication. Instead of sending user credentials over the network, key is created for the user session and used for short limited time. Authentication of the user while using Kerberos is required only one time and once the user authenticated he can access services and applications without the need to log in again. Sign in for each application independently lead to some problem [14]. Authentication process starts with authentication service request (AS_REQ packet) which contains the client username, service name and the current time of authentication request that used by domain controller to make sure that the logon is current and avoid a replay attack. figure 5 shows AS_REQ packet

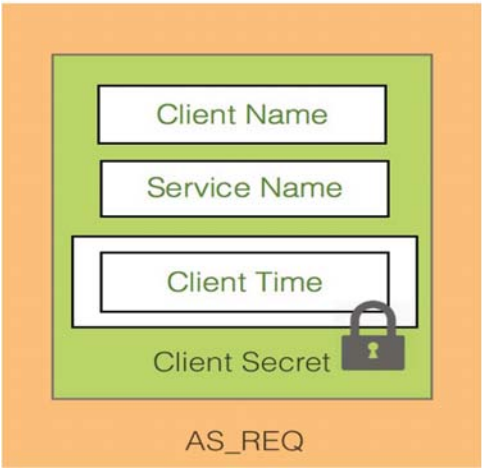


Figure 5: The authentication service request packet

The domain controller is responsible for validating user authentication request [15] and issuing a ticket-granting ticket (TGT) which cached and used by windows, so the user does not have to logon to services again. Authentication service response (AS_REP packet) have TGT encapsulated with it. Figure 6 shows AS_REP packet.

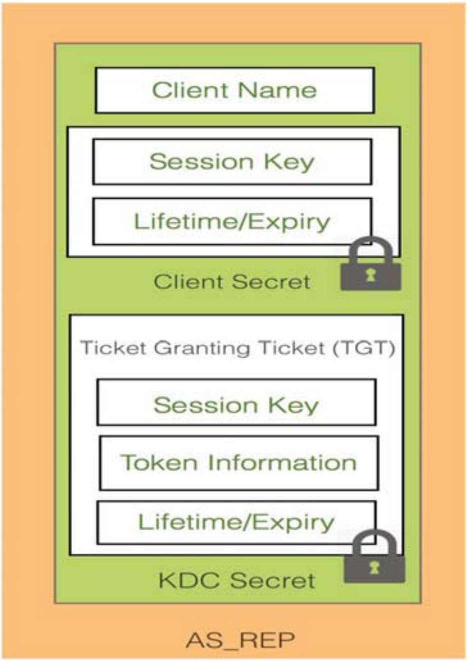


Figure 6: The authentication service response packet

Session key used to communicate with the domain controller. Lifetime /Expiry is a limited period defined by TGT when it expires TGT must be renewed or authentication request must be done again. Session key and lifetime/Expiry are encrypted using user password hash. TGT contain token information which is about user information like his access right, groups he belongs to. TGT encrypted using a hash of the KDC's secret which is the hash of krbtgt account credential for domain controllers [1].

D-Active Directory Availability Group

When we are looking for availability, the newest Azure Active Directory Availability group provide several services that enhance and secure the active directory model. Regrettably, considering availability often be the last step after the project is finished. Azure usually puts the high availability in the top feature need. In azure active directory data are kept in triple redundancy. However, services are not redundant and losing one node can be less expensive than losing one application. This can be done when companies are using failover cluster instances (FCIs) with the provided AlwaysOn Availability Groups feature. Availability groups in Azure serve the following features. Services like Availability sets, which allow working on the data in multiple locations shown in figure 6 Other services like Management services, Notification hubs, AutoScale and Virtual machines [12].

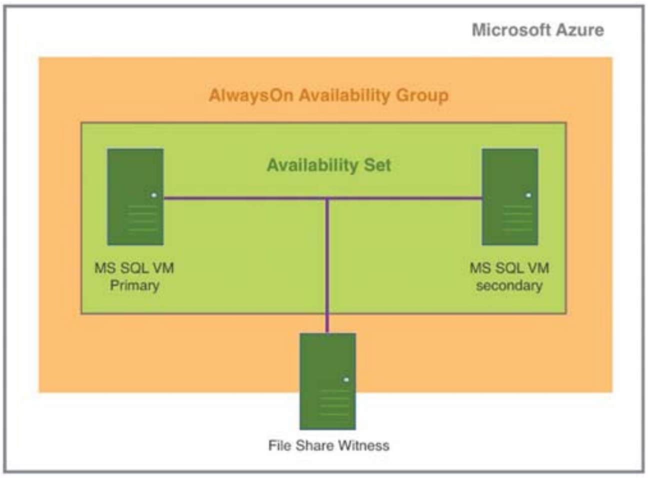


figure 7: Availability groups in Azure, using an availability set.

VI. CONCLUSION

Active directory is a very common solution for any company that wants to control and manage information and resources. It is integrated into windows servers which have some vulnerabilities that could affect active directory in the organization. maintaining the security of windows server enhance the security of active directory. There are different features of the active directory that might raise security concerns if not used properly. Active directory has pre_built in security measures and many capabilities that help in managing security in the organization. securing the environment where the active directory is placed is the responsibility of the company. While this paper discussed active directory as the important system for organization security, there are too fighting chances to make this scope exceed the level that has been reached. Developing a business case for the active directory can be presented in future papers to refine our findings. Comparing and a contrast between active directory and other similar available systems should be encountered. In addition, a plan to implement active directory based on benchmarking can be developed.

REFERENCES

[1] B. Desmond, J. Richards, R. Allen and A. G. Lowe-Norris, *Active Directory*, 5th ed. Sebastopol: O'Reilly Media, Inc, 2013, p. 1-281.

[2] P. Pengsart, A. R. X. Belo, J. X. Vaz, J. B. S. Marques and E. Junior, "ADFS Authentication for Healthcare System," in *International Conference on Information Technology*, Nakhon Pathom, 2017.

[3] G. Tomsho*, MCTS Guide to Configuring Microsoft Windows Server 2008 Active Directory*. 2009, pp. 76-77.

[4] L. Hunter, *Active Directory Field Guide*. Apress, 2005, pp. 149-176.

[5] M. Derek, "REVOLUTIONIZING CONTINUOUS AUDITING OF DIRECTORY", vol. 29, no. 4, pp. 42-44, 2018.

[6] P. C. R. V. Parmi, "An Advanced approach of Active Directory Techniques," *International Journal of Information and Technology (IJIT),* p. 7, 2015.

[7] "Microsoft Windows Active Directory Denial of Service Vulnerability", *Tools.cisco.com*, 2018. [Online]. Available: https://tools.cisco.com/security/center/viewAlert.x?alertId=53262. [Accessed: 05- Feb- 2018].

[8] (MS07-039) VULNERABILITY IN WINDOWS ACTIVE DIRECTORY COULD ALLOW REMOTE CODE EXECUTION (926122) - Threat Encyclopedia - Trend Micro US", *Trendmicro.com*, 2018. [Online]. Available: https://www.trendmicro.com/vinfo/us/threat-encyclopedia/archive/security-advisories/(ms07-039)%20vulnerability%20in%20windows%20active%20directory%20could%20allow%20remote%20code%20execution%20(926122). [Accessed: 02- Feb- 2018].

[9] "Active Directory Certificate Services Vulnerability - oval:org. mitre. oval:def:12749", *Itsecdb.com*, 2018. [Online]. Available: http://www.itsecdb.com/oval/definition/oval/org.mitre.oval/def/12749/Active-Directory-Certificate-Services-Vulnerability.html. [Accessed: 02- Feb- 2018].

[10] "Active Directory Buffer Overflow Vulnerability - oval:org. mitre. oval:def:14037", *Itsecdb.com*, 2018. [Online]. Available: http://www.itsecdb.com/oval/definition/oval/org.mitre.oval/def/14037/Active-Directory-Buffer-Overflow-Vulnerability.html. [Accessed: 02- Feb- 2018].

[11] S. Metcalf, "The Most Common Active Directory Security Issues and What You Can Do to Fix Them – Active Directory Security", *Adsecurity.org*, 2018. [Online]. Available: https://adsecurity.org/?p=1684. [Accessed: 03- Feb- 2018].

[12] M. Copeland, J. Soh, A. Puca, M. Manning, and D. Gollob, *Microsoft Azure: planning, deploying, and managing your data center in the cloud:* New York: Apress, 2015.

[13] D. J. R. K. Jaroslav Kadlec, "Implementation of an Advanced Authentication Method Within Microsoft Active Directory Network Services," in *2010 Sixth International Conference on Wireless and Mobile Communication*, Brno, 2010.

[14] H. Wang and C. Gong, “Design and Implementation of Unified Identity Authentication Service Based on AD,” *2016 8th International Conference on Computational Intelligence and Communication Networks (CICN)*, 2016.

[15] C.-M. L. C.-H. M. a. T.-C. K.-C. L. Chih-Hung Hsieh, "AD2: Anomaly Detection on Active Directory Log Data for Insider Threat Monitoring," in *2015 International Carnahan Conference on Security Technology (ICCST)*, Taipei, 2015.