ISSN 2347 - 3983
Volume 8. No. 5, May 2020
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter80852020.pdf
https://doi.org/10.30534/ijeter/2020/80852020

Ensuring Network Security using Secured Privileged Accounts

I.Jeena Jacob[1], Dayanand Lal.N[2], Parikshith Nayaka S K[3], Beena G. Pillai[4], Nida Kouser[5]
[1]Assocate Professor, Department of CSE, GITAM School of Technology, Bengaluru, India
[2-5]Assistant Professor, Department of CSE, GITAM School of Technology, Bengaluru, India
[1] jeni.neha@gmail.com, [2 2]dayanandlal@gmail.com, [3] pari2sn@gmail.com, [5] itzme.nida@gmail.com

ABSTRACT

Every organizations pay lot for securing their information because of the attacks. The evaluation of the business need against best practices should be made to monitor and protect privileged accounts. Best practices should be formed to protect privileged accounts since attackers will try all the means to exploit privileged accounts. Many professionals have tried different ways to secure the organization from the attacks. This paper proposes the ways to securing privileged accounts by analyzing the windows active directory. This gives the ways to do the vulnerability assessment and ensuring the security. The performance analysis shows that the proposed scheme works well in the given enterprise data.

Key words: Privileged accounts, Active directory, Privileged Access Workstation.

1. INTRODUCTION

Because of the existence of internet and computers, past few years witness simple or complex attacks against computing infrastructure. As the number of industries and organizations increasing, the attacks in cyber space significantly change its landscape. Usually the main target of the attackers is large companies or organizations. So, the privileged accounts of every organizations should be secured safely because it is exploited to attacks more often. The security frameworks like NIST and Council on Cyber Security also ensures the importance of securing privileged accounts since these accounts hold the keys for that organization's digital kingdom [1].

Microsoft created a technology named Active Directory (AD) for providing various services like authentication, accessing and LDAP directory services. Active Directory is a database which stores the vital information like services and applications which can be used to access needed information. Usually system administrators use this directory for ensuring security by utilizing the stored information [2]. Many studies were done to check the source of attacks [17] and to check at which time the attacks were find out [18]. The reports of Verizon say because of external actors, 80% of advanced attacks happen [17]. Many security systems [20,21] are proposed in various application areas. This paper proposes the feasible ways for protecting the privileged accounts in AD environment.

2. RELATED WORK

Many researches were done to reduce the attacks to Active Directory. The researches [3] say the possibility of preventing these attacks is very less, but the trials can be taken for reducing it. Sean [4] discusses about the Active Directory and about the security measures to be taken by a security professional. Another research [5] says about the three phases to secure privileged accounts. Another work [6] also tells about the security measures to be taken for security AD. The trusts that should be maintained by the AD [7-9] also discussed by many professionals. The securing of AD can also be done by replicating the AD [10-12]. Some argues that when code is closed for proprietary programs, those cannot be used by the hackers. When it is closed, they cannot access the holes by security by obscurity [13].

Another way of preventing the attacker is detecting the attacker earlier. This will aid to prevent the more damage that will cause in the network because of long time existence. The attacker can be stopped before gaining full control [14]. The attacking can also be reduced by providing proper access control. Little thinking should be done when the access control is provided. When the access privileges are provided for directory, sensitive assets, domain controllers and domain administrative privileges, it should be done carefully [15]. Administrative model control restrictions can also be given for AD in tiered model [16]. Advanced Threat Analytics (ATA) [19] is a software which can detect the group modification activities of users and also can alert the system when any abnormality occurs

3. PROPOSED WORK

This paper gives the ways to deploy windows privileged accounts protection by using a number of sources. The work is done with the production environment data which contains

thousands of sensitive data. This work shows and explains the effectiveness of implementing some security measures by joining built-in resource in Windows with open source software. This is done in many steps.

3.1. Preliminary Stage

Organizations are responsible for managing their privileged accounts in Windows AD environment. The first step in giving security is by enforcing recommended privileged access security. These practices need only changes in processes. The actions which give better outcome should be selected. Measure should be taken to keep less number of privileged accounts because safeguarding the accounts safe in the environment is critical. When the system is set up, the accounts should be checked and reviewed. The very much needed privileged accounts should be kept live and unnecessary accounts should be deleted. This will help the management to reduce the management cost.

An employee can be given with two different accounts which will help to reduce the risk while the attacker tries to attack the system through employee login. Automatically it helps the organization to be safe from the attack because most of the attacks happen when the user tries to access e-mail for an instance. Other security measures to be taken are: giving least privileged names for standard user accounts, storing password securely, creating a process for registering on- and off-boarding employees of those who have privileged account access.

3.2. Creating active directory delegation model

Based on the directory formed in preliminary step, an active directory delegation model is formed. It is formed by creating role-based access control, tier model, dealing with tier-0 groups, forming secondary account, privileged admin workstation, creating naming convention and cleaning privileged accounts.

3.3. Detecting environmental vulnerability to privileged accounts

In order to detect the AD environment that might be exposed to the risk, the vulnerability assessment should be done. The small industries which will not have many privileged accounts are subjected to this kind of assessment effectively. The bad AD design can be identified by analyzing administrative model, naming convention, lack of monitoring and redundant data.

3.4. Role based access control

Role-based access control (RBAC) is an access control which is used to give the permission based on its role. These roles will decide to which extent access of network can be given. The four components are users, roles, permissions and objects. Also the roles like primary, billing, technical and administrative also may be given.

3.5. Tier model

Different tiered network can be given as the next step. The tier model will help the organization to safeguard the identity between full control of the Tier 0 and the high-risk workstation assets. Tier 0 is called as forest admins which gives administrative control of the active directory. Tier 1 is called as server admins which gives the administrative control over a single or multiple server. Tier 2 is called as workstation admins which gives the administrative control over a single or multiple device. Figure1 gives the tiered architecture.

Figure 1: Tiered Architecture

3.6. Privileged Access Workstation (PAWs)

PAW is used for providing a dedicated operating system to give provision for sensitive tasks which is protected from attacks. This will help to separate the sensitive deeds and accounts from phishing attacks and OS vulnerabilities. PAW will help to implement privileged credentials which are not exposed on standard clients, to maintain credential exposure contained to the same trust level and enabling tight security controls.

3.7. Giving proper naming convention

Standard naming should be given for every company. The names can be formed by level of access, level of security, type of resource, etc.

Syntax: Role-<Role Tier>-<Role Name>

Example: Role-T2-WorkstationAdmins [16].

4. IMPLEMENTATION DETAILS

The implementation and analysis of this work is investigated in Swedbank's infrastructure. The whole security practices needed for the best windows privileged accounts and the solutions were implemented and analyzed. The open source software named Zabbix is used. Zabbix gives visually intuitive and configured details along with specific documents. Zabbix will also give the graphs and statistical

information. The same solutions can be applied for any AD infrastructure because of its flexibility.

The privileged groups in tier 0 has windows AD security. There are some other groups also there which are sensitive. And require more permission to perform actions in AD. So the information should be gathered about privileged accounts. The AD may contain different information like the current device location, its configuration, its impact etc. From the security point of view, this information will give the importance of these on Windows AD infrastructure. Domain admins' security group members only can administer the domain. They will be the default owner for the objects present in Active Directory. Figure 2 provides the way to execute Tier0AccountGathering.

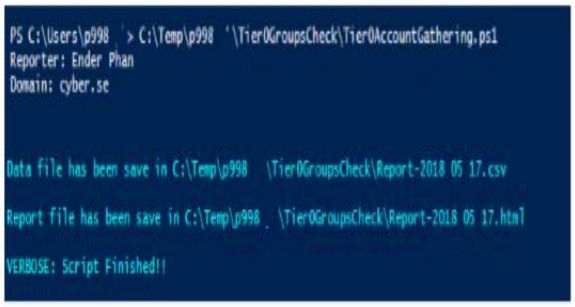

Figure 2: Tier0AccountGathering gets executed

Two files will be exported after execution as in Fig.2. Fig.3 gives the reports. These two files which have account information will be saved in csv format and also the report in html.

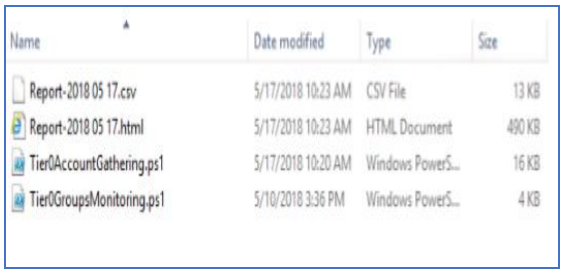

Figure 3: Reports are exported

These reports which are in CSV format will be useful for the investigators to identify the fields that are interesting to them. The reports will provide various information which can be used for taking the decisions. These web page results are written in HTML and CSS. Fig.4 gives the percentage of expired accounts. Fig.5 gives the status of enabled and disabled accounts. Fig.6 gives the necessity of account which need password. Fig. 7 gives the information about the never changed password. Figure 8 gives the last changed password information.

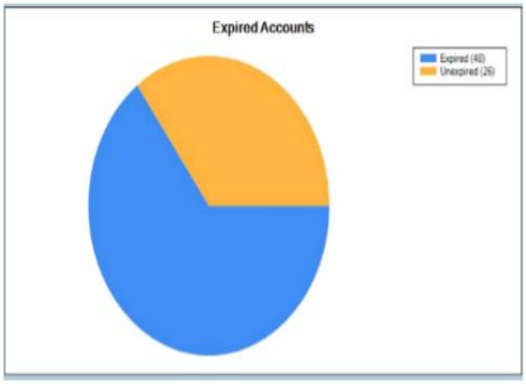

Figure 4: Expired accounts in pie chart.

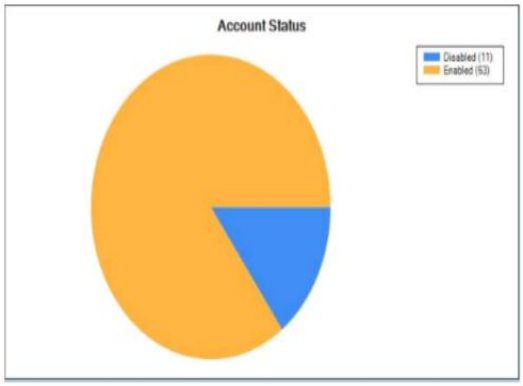

Figure 5: Status of enabled and disabled accounts.

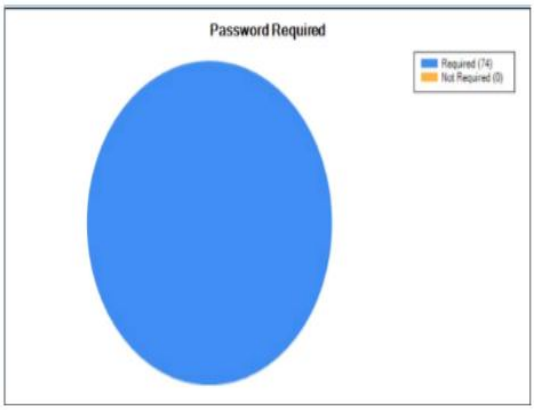

Figure 6: Status of Required Password

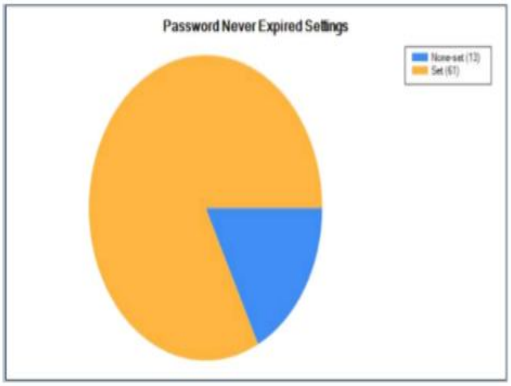

Figure 7: Password which never changed

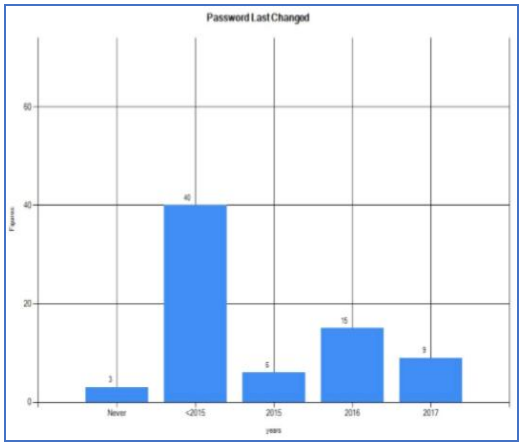

Figure 8: Last changed password information

These analyses give us the information regarding different security measures and its flaws. Figure 8 tells when password was changed the last time. As per this figure, there are 3 accounts which never changed its password. This is not advisable. The passwords of privileged accounts should be changed often at least once in a month for preventing attacks. The scenario of this figure is not a good sign because more than 88% accounts have not changed their password before 2017. Based on these kinds of analyses the decision should be taken to the measures to be taken for securing the system.

5. CONCLUSION

The protection of privileged accounts decides the existence of all organizations. This proposed work gives the steps to ensure the security in the organization. Also, the proposed work gives the usage of Windows AD for ensuring the same. The analysis done in the Swedbank's infrastructure using open source software named Zabbix provides better results than the other existing works.

.

REFERENCES

1. CyberArk,l**p.cyberark.com**,[Online]. Available: https://lp.cyberark.com/rs/cyberarksoftware/images/wp-securing-privileged-accountsbest-practice-guide-04-15-2014-en.pdf
2. J. Reis, **learnthat.com**, [Online]. Available: http://learnthat.com/introduction-toactive-directory/.
3. Microsoft, **docs.microsoft.com**, 31 05 2017. [Online]. Available: https://docs.microsoft.com/en-us/Windows-server/identity/ad-ds/plan/security-bestpractices/reducing-the-active-directory-attack-surface.
4. Sean Metcalf, **Beyond the MCSE: Active Directory for the Security Professional**, https://www.blackhat.com/docs/us-16/materials/us-16-Metcalf-Beyond-The-MCSE-Active-Directory-For-The-Security-Professional-wp.pdf
5. **The Three Phases of Securing Privileged Accounts: A Best Practices Guide**, https://www.cyberark.com/resource/three-phases-securing-privileged-accounts-best-practices-guide/
6. **Securing Active Directory – An Overview of Best Practices** https://technet.microsoft.com/en-us/library/dn205220.aspx
7. **Active Directory Domains and Trusts** https://technet.microsoft.com/en-us/library/cc770299.aspx
8. **Trust Types** https://technet.microsoft.com/en-us/library/cc775736(v=ws.10).aspx
9. **Understanding Trust**s https://technet.microsoft.com/en-us/library/cc736874(v=ws.10).aspx
10. **How Active Directory Replication Topology Works** https://technet.microsoft.com/en-us/library/cc755994(v=ws.10).aspx
11. **Active Directory Replication Overview** https://technet.microsoft.com/en-us/library/cc961788.aspx
12. **How the Active Directory Replication Model Works** https://technet.microsoft.com/en-us/library/cc772726(v=ws.10).aspx
13. C. Tozzi, **www.channelfutures.com**, 25 July 2016. [Online]. Available: http://www.channelfutures.com/open-source/reasons-organizations-opt-not-use-opensource-software.
14. Microsoft, **cloudblogs.microsoft.com**, 22 08 2017. [Online]. Available: https://cloudblogs.microsoft.com/Windowsserver/2017/08/22/now-available-Windowsserver-2016-security-guide/.
15. R. Smith, **www.petri.com**, 24 October 2017. [Online]. Available: https://www.petri.com/use-microsofts-active-directory-tier-administrative-model.
16. Microsoft, **docs.microsoft.com**, 10 12 2016. [Online]. Available: https://docs.microsoft.com/en-us/Windows-server/identity/securing-privilegedaccess/securing-privileged-access-reference-material.
17. arubanetworks, **www.arubanetworks.com**, [Online]. Available: http://www.arubanetworks.com/assets/so/SO_UEBA_UseCase_CompromisedUsers.pdf.
18. Kaspersky, **www.kaspersky.com**, unknow unknow unknow. [Online]. Available: https://www.kaspersky.com/blog/incident-response-report/.
19. Microsoft, **docs.microsoft.com**, 05 06 2018. [Online]. Available: https://docs.microsoft.com/en-us/advanced-threat-analytics/suspicious-activity-guide.
20. Siva Sankar.D, Vinod Reddy.S, Adarsh.B, Prabu.M, **Implementation of Eco-Friendly Transport System by Using Arduino Solenoid**, GSM Module & RFID Card Reader, *International Journal of Emerging*

Technologies in Engineering Research (IJETER),, Volume 6, Issue 11, November (2018)

21. D. J. Joel Devadass Daniel, Dr. S.Ebenezer Juliet, **A Survey on Security Issues in IoT, ,** *International Journal of Emerging Technologies in Engineering Research (IJETER)*, Volume 7, Issue 12, December (2019)
22. Fuzzy logic based proportional integral control of frequency for small, International Journal of Advanced Trends in Computer Science and Engineering, 2020, volume 9, number 2, pages 1275-1279 Ramaswamy, K. and Dayanand Lal, N. and Parikshith Nayaka, S.K. and Venna, R.C. and Brahmananda, S.H
23. Effective and Secure Approach for Multi-Keyword Quest Graded over Authenticated Data, International Journal of Advanced Trends in Computer Science and Engineering, 2020, volume 9, number 2, pages 2278-3091, Shobharani D, Parikshith Nayaka S K, Swasthika Jain T, Dr. Dayanand Lal
24. Mr. Parikshith Nayaka S K, Mrs. Shobha Rani, Dr. Dayanand Lal, Dr. M Anand. (2020). Convert Channel and Information Hiding in TCP/IP . *International Journal of Control and Automation*, *13*(02), 582 - 591. Retrieved from http://sersc.org/journals/index.php/IJCA/article/view/11199