Vol 11, Issue 4 , April/2020
ISSN NO:0377-9254

Implementing Active Directory and Information Security Audit also VAPT in Financial Sector

Kajol Patel[1], Dr. Priyanka Sharma[2]

[1] Student, M.Tech in Cyber security at School of Information Technology & Cyber Security, Raksha Shakti University, Lavad, INDIA

[2]Professor and Director (Research & Development), School of Information Technology & Cyber Security, Raksha Shakti University, Lavad, INDIA

***Abstract*— Digital world has opened unlimited avenues of opportunity by enabling organizations to conduct business and share information on a global basis. Active Directory Domain provides information about network resource such as users, user's password, groups, authentication process, network printer and computer and makes the information available to computer users and administration. Active directory allows administrator to manage centrally all management with the help of group policy. However, it has also brought new levels of security concerns for consumer's private information in financial sector. Also this paper describes brief techniques involved in Vulnerability Assessment and Penetration Testing (VAPT) which helps to infrastructure security which is installed by the banking sector to remain protected from the Cyber world threats. The presence of an information security audit increases the probability of adopting major security measures and preventing these attacks or lowering the cyber world attacks. Main objective of this paper at creating high level of Cyber Security awareness and importance at all levels of financial sector, Organization, enabling them to adopt required up-to-date security measures and remain protected from various Cyber-attacks. In this project, integrating these AD Services aids system administrators by providing a single tool to manage multiple components of AD.**

Keywords*— *Active directory (AD), AD services, Information security, financial sector, VAPT.

1. INTRODUCTION

The Active directory providing the knowledge about objects, organizing the objects, access management and sets for security view aspects. AD domain has the services to store data concerning the network resource across a web site. AD structure has the hierarchy framework of objects. the objects falls into 3 main classes resource, service, user(accounts or user and group).Before this AD, Windows server has long-faced complication like, authentication and authorization model needed breaking down a network into domains, and generally, unpredictable system ways that of trusts. AD uses protocols likes LDAP, Kerberos version, and DNS version. Domain controller of active directory authenticating and authorized the all ad users throughout a particular windows domain network and additionally distribution and implementing security policies for all computers and putting in or change software package. as an example, once a user logged into a system that's a vicinity of a domain and AD will checks the submitted username, word and determines whether or not the admin user or traditional user.

An audit structure could be a set of documents and that specifies the strategy of the audit method, the expected audit's concludes, identifies the danger management method, and additionally risk assessment. Moreover, the audit structure ought to contain a step by step instruction on a way to prepare a particular audit strategy. It'll embrace a way to gather the specified info, awareness, employees' interviews, reviewing the results of previous audits, selecting the audit strategy methodology and tools that may be valid perform on a particular audit. the aim of the audit structure is delivered as audit reporting back to the organization's chief executive officer and Board of Directories, these audit reports can embrace the audit's strategy results supported proof and conclusions.

Although financial sector can be secure by various ways wherein Vulnerability Assessment and Penetration Testing (VAPT) process is a special approach to secure and aware from both logical and wide range of technical vulnerability and awareness. This approach information security audit in financial sector also can be used to secure associated layers. VAPT includes auditing the system for finding loopholes, which may be exist on the system, exploit that loophole same as an attacker perspective and produce data which representing the system level risk.

The Analysis of the IS audit has finished that the massive organizations or banking sector will implementing AD in their system, that the main goal of this analysis supported auditing expertise with banking sector and therefore the vital role of active directory in managing users and resources of the massive organization and maintaining acceptable levels of security within the system. during this paper, the second section delineate vulnerabilities of active directory servers. The third section describing the safety of active directory that is alert feature, maintaining the integrity and confidentiality in active directory networking, user authentication in active directory and active directory accessibility cluster into the actual system. This cyber security fields currently increasing day by days thus for that everyone massive organizations have to be compelled to implements some forms of security mechanism, that makes them secure.

2. LITRATURE SURVEY

In 2016, Kamran Shaukat, Amber Faisal, Rabia Masood , Ayesha Usman, Usman Shaukat5 et al surveyed completely different frameworks which can be secure at the testing level. they have projected AN entrance testing technique to secure the databases, networks, net applications and automaton within the monetary sector. In context of entrance testing throughout their technical aspects review, known by that studied approaches helpful to specific frameworks and not every ways are often Appling to explicit framework and issues as neglecting it. to beat these problems, they have tried and projected another methodology and explaining all the parts in their paper.

In throughout this year, Jai Narayan Goel1 et al, Mohsen Hallaj2 Asghar et al3, Vivek Kumar4 et al, Sudhir Kumar Pandey5 et al propose AN Ensemble approach with varied VAPT tools that reliable in prediction of vulnerability for the aim of decreasing the false positive. they have additionally enforced their ideas and created a code supported their strategy referred to as “VEnsemble one.0” that's employed with style of each open supply and business tools and enclosed the results.

In 2016 year, Prashant S. Shinde1 et al, Shrikant B. Ardhapurkar2 et al explained clearly of various aspects and techniques employed in vulnerability assessment and penetration testing. Additionally concentrate area on cyber security threats awareness and importance in organization, monetary sector to stay safe. They conclude that there unit several tools obtainable for VAPT, with new vulnerability evolution existing tools must be upgraded to identify new vulnerabilities and makes them versatile and reliable so new attack signature are often known.

In 2017, S. Sandhya1 et al, Sohini Purkayastha2 et al, Emil Joshua3 et al, Akash Deep4 et al discussing the utilizing the penetration testing approach exploitation Wireshark tool and demonstrating that technique. It have additionally survived many tools for penetration testing to unravel security aspects and problems.

In 2016, Subarna Shakya1 Abhijit Gupta2 discussing the audit aspects and challenges on system and Security Audit areas. additionally they seeks clarification from the perceptive the problems or behavior. group action Controls unit such techniques and issues that addressing group action security and focus on risk management and laptop security of the program at intervals the monetary sector and organization.

In 2015, P. C. R. V. Parmi1, discussing and implement the thought of active directory in giant organizations may face to the loss of management over user's resources and knowledge which may lead to serious security threats. Directory which is ready to then create the replication of all domain controllers within the domain. However option to store the DNS info within the AD is not obtain on DNS servers that is not a domain controller.

3. METHODOLOGY

The requirement of protocols in active directory, First methodology LDAP could be used by users to search and locate a particular object like any system. LDAP makes use all keywords to carry out a search operation. The identities of the objects are done with the help of its attributes. Second methodology DNS that are domain controllers it will store the data of the AD which will then make the replication of all domain controller of the particular domain. Third methodology for All AD domain are KDCs, They might also be file servers so make them Kerberos servers. We might also log on to a domain controller's console and attempt to access files on another server, in which case the domain controller becomes a Kerberos client.. So for Kerberos protocol, it’s important to consider what role each participant is authenticating with single particular authentication transaction. The authentication protocol strategy of the active directory methodology is shown in Fig.1 and Fig.2.

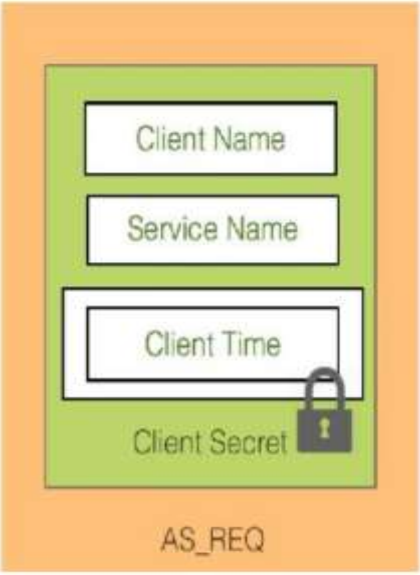

Fig 1. Authentication protocol process

User's access to network resources is controlled through logon method wherever the user should give his or her papers to make an access to services and application. This protocol provides versatile authentication mechanism. Rather than causation user credentials over the network secret's created for the user session and Used for brief restricted time. The domain controller for supportive has responsibility for user authentication request and issued a price ticket} granting ticket (TGT) that cached and employed by windows, that the user doesn't have to be compelled to logon to services once more. Authentication service response (AS_REP packet) has TGT encapsulated with it. The figure below shows AS_REP packet.

Session key used for communicate with the domain controller. life|period of time|period} /Expiry may be a restricted period outlined by TGT once it expires TGT should be revived or authentication request should be created once more. Session key and lifetime/expiry is encrypted victimization user word hash. TGT contain token data that is concerning user data like his access right, teams he belongs to. TGT encrypted employing a hash of the KDC's secret that is that the hash of krbtgt account papers for domain controllers. This protocol is wide spreads for the safety mechanism.

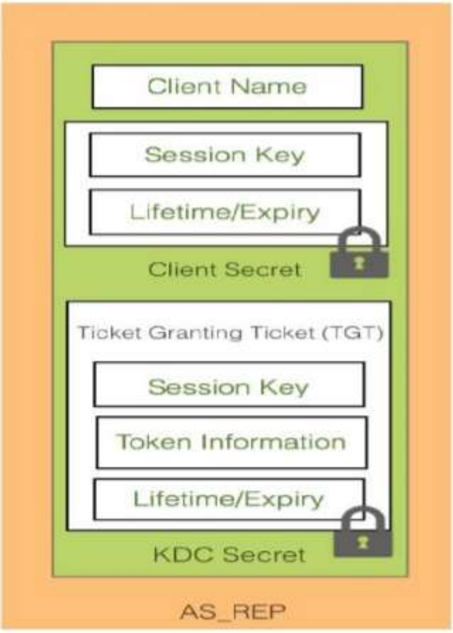

Fig 2. Authentication protocol process 2

Forth methodology for Multi factor authentication, User account is less likely to be compromised if user uses the multi factor authentication. It will provided by organization's active directory services. and it provides multiple ways to enabled this service in n AD own services . The process of multi-way factor authentication is described in Fig 3.

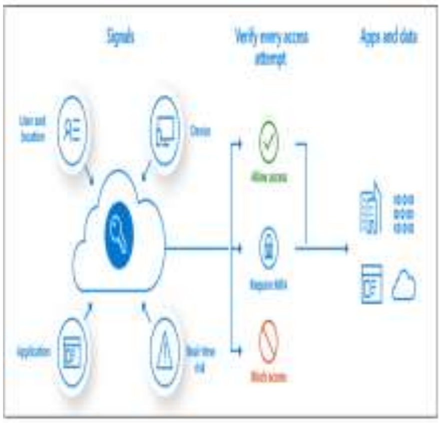

Fig 3. Multi-factor authentication process

4. VULNERABILITY ANALYSIS

4.1 Service Account has Over-permission

In service accounts has kind of account that always provides a lot of privileges and allow services to the superjacent the actual software package. This services running beneath service incorporates a certificate in LSASS (Local security authority subsystem) which might be purloined and extracted by the offender and if the purloined credentials has admin rights then it'll be simply compromises the whole IT infrastructure.

4.2 Initial breach targets

Most of data security breaches begin with the compromising the little organization's infrastructure, usually one or 2 systems at a particular time. These initial steps or entry points into any network, usually exploit vulnerabilities that might are fastened. Usually seen vulnerabilities are:

- Gaps in between antivirus and antimalware deployments
- Incomplete patched system.
- Outdated applications and operational systems
- Misconfiguration of system.
- Lack of best secure application practices

4.3 Activities that will increase and compromised

Attacker largely targets the extremely privileged domain accounts and important person accounts, it's necessary for admin to be serious activities that increase the foremost of a hit of a purloined the certificate.

- Logged on to unsecured computers with privileged accounts.
- Browsed the net with a extremely privileged account.
- Configure native privileged accounts with an equivalent credentials across systems.
- Overpopulated and overused of privileged domain teams.
- Insufficient management of the safety of domain controllers at intervals implementation.

4.4 Privilege Elevation and Propagation

Specific accounts, servers and infrastructure elements area unit typically the first targets of attacks against domain. Other infrastructure services that affected to identity, access and configuration management, like public key infrastructure servers and systems management servers.

5. ATTACK VECTOR

5.1 The Privileged Accounts and teams in AD

Discussed the high privileged user accounts and teams in AD and also the mechanisms by that privileged user account is protected. At intervals AD 3 inbuilt teams are the best privilege teams within the directory (Admin), through variety of extra user teams and user accounts ought to even be protected.

5.2 The Implementing Least-Privilege body Model

It known the chance that the utilization of high privileged user accounts for every day admin presents, additionally to providing suggested to cut back it risk.

Excessive privilege isn't solely found in AD in compromising setting. It's generally found within the infrastructure:

- In Active Directory
- On member services
- On workstations
- In Applications
- In Knowledge repositories

5.3 The Implementing Secure Admin Hosts

Secure admin hosts, that computers configuring to support body of AD and connecting systems. These host is dedicated to body functioning and don't run software system like email applications, internet browsers, or productivity software system.

Included during this section describes the following:

- Never admin a trusty system from a less-trusted host.
- Do not have confidence one authenticating issue once perform privileged activities.
- Do not forget the physical security designing and implementing for secure admin hosts.

5.4 Securing Domain Controllers against attack

If Associate is as attacker and getting privilege, that attacker will tamper, corrupt and destroy the AD information, and by extension, all of the systems and user accounts that managed by AD.

5.5 Physical security provides for domain controllers

It contained recommendation for providing physical internal security for the domain controller mechanism in datacenters, head offices, branch offices, and remote locations.

5.6 Domain controller operational systems

It contains recommendation for securing the domain controller operational systems.

5.7 Secure Configuration for Domain controllers

It freely on the market configuration tools and it is enforced by cluster policy objects.

5.8 DCshadow attack on AD

In DCshadow attack, it detects the rogue domain controller replicating malicious changes to AD.

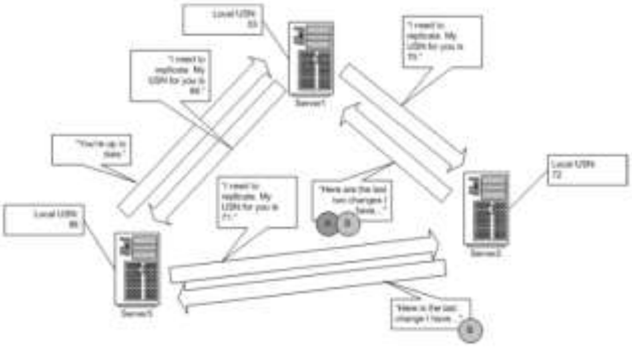
Local USN
"I need to replicate. My USN for you is"
"You're up to date"
"Here are the last two changes I have."
"Here is the last change I have."
Server1

Fig 4. Propagation dampening in AD replication

A DCShadow attack on AD and it is design for change the directory using malicious replica of objects. During this attack, DCShadow impersonating the Domain Controller using admin rights and starts a replication process, so that changes made on one DC are synchronizing with other DCs. DCShadow creates the replication of directory Service Remote Protocol and AD Technical specification.

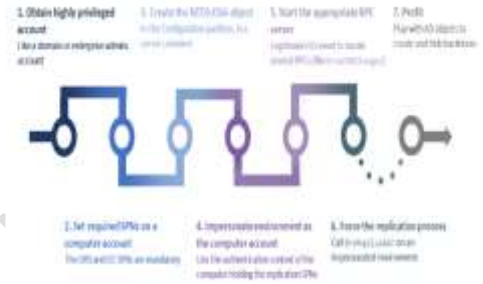
1. Obtain highly privileged account
2. Set required SPNs on a computer account
4. Impersonate environment as the computer account
7. Profit

Fig 5.Rogue Replication Flowchart

That is not a way to do privilege escalation. It already needs to be part of the host Admins or organization Admins group, or some high authority as it will need the rights to “register you as a new member of the replication process”.

But once you get there, attacker can use DCShadow to further work on domain area, modify AD without being noticed by SIEM systems, and use it as a way to gain valid user's access. There is main limit point of an attacker to attack is the impossibility for to inject new vulnerable code in the targeted AD domain.

6. RESULT AND DISCUSSION

The process of DCshadow attack is shown in Fig 6, Fig 7, Fig 8.

Fig 6. Lateral movement feature

Fig 7. Show incidents

Configured The Defender security for DCShadow Attack.

Microsoft’s provided new intelligent security graph, these ATP services connect together and provide a clear view of your environment. You can pivot from your organization ATP’s identity-centric view to Windows Defender ATP’s machine- & user-side views and vice versa. This way you can track an attacker’s lateral movement in this feature.

Fig 8. Rogue replication

7. CONCLUSION

For existing system, in financial sector there would many vulnerabilities occurred due to access privileges mechanism. So for the best solution is to implement active directory environment and performing information security audit for financial sector and it can provides the help from the inside and outside cyber-attacks.

ACKNOWLEDGMENTS

I am indebted to my superior, Professor Dr. Priyanka Shrama she convincingly guided and encouraged me to be professional and do the right thing for the research paper. Without her persistent help, the goal of this paper will not have been realized.

REFERENCES

[1] Implementation in an Advanced Authentication Method Within Microsoft Active Directory Network Services,by D. J. R. K. Jaroslav Kadlec,

[2] http://doece.pcampus.edu.np/index.php/prof-dr-subarna-shakya/

[3] https://www.morganclaypool.com/doi/abs/10.2200/S00240ED1V01Y200912DMK002

[4] https://docs.microsoft.com/en-us/security-updates/SecurityBulletinSummaries/2007/ms07-jul

[5] https://www.researchgate.net/publication/335803762_Cyber_Defence_A_Hybrid_Approach_for_Information_Gathering_and_Vulnerability_Assessment_of_Web_Application_Cyberdrone

[6] https://www.vutbr.cz/vav/projekty/detail/18799

[7] http://icil.uniroma2.it/wp-content/uploads/2019/06/The-Support-of-Strategy-Consulting-To-Italian-SMEs-In-Regaining-Competitiveness-in-the-IT-Sector.docx

[8] https://ieeexplore.ieee.org/document/8014711/?section=abstract

[9] https://www.researchgate.net/publication/254004698_Mitigating_Program_Security_Vulnerabilities_Approaches_and_Challenges