INTERNATIONAL JOURNAL OF LATEST TECHNOLOGY IN ENGINEERING, MANAGEMENT & APPLIED SCIENCE (IJLTEMAS)
ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue IV, April 2024

Penetration Testing Platforms for Active Directory Network Environment

Oluyomi Kolawole Akinyokun[1], Oyefunmke Adeninhun Famose[2]

[1]*Department of Cyber Security, Federal University of Technology Akure, Ondo State, Nigeria,*

[2]*Academic Planning Unit, Federal University of Technology Akure, Ondo State, Nigeria*

DOI: https://doi.org/10.51583/IJLTEMAS.2024.130402

Received: 26 February 2024; Accepted: 20 March 2024; Published: 28 April 2024

Abstract: The security of Active Directory environments is a crucial aspect for organizations of all sizes. With the increasing number of cyber threats, it is important to understand the different penetration testing paradigms that can be used to attack these environments. This research focuses on a comparative analysis of four specific attacks: LLMNR poisoning, SMB relay, pass the hash, and token impersonation. The comparison is based on relevant criteria such as complexity, required tools, and susceptibility to defense mechanisms. The primary objective of this study was to build a virtual Active Directory network, which provides a controlled environment for testing the different attacks. This enabled us to evaluate the effectiveness of each attack and gather insights into the strengths and weaknesses of each paradigm. By conducting a comparative analysis using these criteria, we were able to determine the most effective methods for defending against these types of attacks and identify areas for improvement. The results of this study provide valuable insights into the security risks that organizations face when it comes to Active Directory environments. By understanding the different strengths and weaknesses of each attack, organizations can make informed decisions about which mitigation strategies to implement. This research also highlights the importance of continuous monitoring and testing to ensure the security of Active Directory environments. This comparative analysis provides a comprehensive overview of four key penetration testing paradigms for Active Directory environments. The results of this study can help organizations to better understand the security risks they face and implement effective mitigation strategies.

Keyword: Penetration Testing, Active Directory, comparative analysis, Vulnerability, LLMNR poisoning.

Introduction

Conceding the increasing importance of information systems in today's complex virtual environment, an organization must perform a high level of diligence to ensure the confidentiality, integrity, and availability of digital resources and users' information. To prevent different types of attacks from malicious users from occurring in the future, this paper proposed a comparative analysis of the penetration testing paradigms for Active Directory network environments in an organization.

Penetration Testing is the process of finding security vulnerabilities in a target environment that could let an attacker penetrate the network or computer systems [20]. A Penetration test can assess both IT Security and the security of the facility where the IT systems are located. If the penetration tester assesses the IT security, the goal is to obtain or modify confidential data located deep into the organization. Penetration testing is very important for network infrastructures as it takes care of confidential data. It ensures that confidential data does not get overlooked by an unauthorized entity. It works beyond the black box and white box testing. Security testers may use many techniques to locate the system's vulnerabilities [11].

Security is a moving target that is effectively managed with a continued lifecycle approach. There are different new malwares, new vulnerabilities, changes in the organizations, and new technologies being implemented. Active Directory is used by over 90% of the Fortune 1000 Companies in the world to manage their network resources efficiently [1] and therefore they must understand how to secure them effectively and take recommendations into account to correct the most critical vulnerabilities discovered during penetration test as much as possible. Some fixes can also be integrated into functional and technical development projects or implemented on the systems with similarities with the target of penetration testing.

In this research, a comparative analysis was performed to evaluate the various penetration testing paradigms for active directory environments. The objective was to build a virtual active directory network and evaluate the effectiveness of four common attacks, namely LLMNR poisoning, SMB relay, Pass the Hash, and Token Impersonation. The project aimed to compare these attacks based on the criteria of the number of tools required, level of detection, and defensive mechanisms. The results of the comparative analysis will provide valuable insights into the strengths and weaknesses of different attack methods, and help organizations to better understand the measures they can take to protect their Active Directory environment. By performing a comprehensive analysis, this project will contribute to the field of cybersecurity and provide valuable information for organizations looking to secure their Active Directory environments.

Literature Review

A. Penetration Test

A penetration test, also known as a pen test, is a simulated cyber-attack against your computer system to check for exploitable vulnerabilities [9]. Penetration testing is a controlled provisional to infiltrate into a framework or system with a specific end goal to recognize vulnerabilities. The type of penetration testing normally depends on the scope and the organizational wants and requirements.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue IV, April 2024

In black box penetration testing, the tester has no idea about the systems that he is going to test. He is interested in gathering information about the target network or system. Whereas, in white box penetration testing the tester has been provided with a whole range of information about the systems and/or network such as System Architecture, Source code, OS details, IP address, etc. It is normally considered a simulation of an attack by an internal source, In the Grey box penetration testing a tester usually provides partial or limited information about the organization's internal details. It can be considered an attack by a hacker who had gained illegitimate access to an organization's network infrastructure documents.

B. Active Directory

The Active Directory (AD) is a centralized authentication and authorization system used in many organizations. It provides a centralized management for user accounts, computers, and other resources within a network. Due to its critical role in ensuring the security of an organization's digital infrastructure, the AD environment has become a popular target for cyber-attacks. Active Directory is the most commonly used identity management service in the world i.e., 95% of fortune 1000 companies implement the service in their networks

Active Directory provides several key services, including Domain Services, Certificate Services, Federation Services, and User's Rights Management. Domain Services provide the core authentication and authorization services for an Active Directory environment. It is responsible for validating users' identities, managing user and computer accounts, and enforcing access policies. Certificate Services allow organizations to manage and issue digital certificates, which are used for secure communication and authentication. Federation Services provide a mechanism for securely sharing resources and user information between different organizations, such as between two separate companies. User's Rights Management Services provide a way to protect sensitive information by controlling how it is used, even after it has been shared with others.

The logical components of Active Directory include the domain, tree, and forest. The domain is a collection of objects such as users, computers, and resources that share a common namespace and security boundary. The tree is a collection of one or more domains that share a common namespace, but have different security boundaries. The forest is the highest level of organization in Active Directory, and is a collection of trees that share a common schema, configuration, and global catalog.

The physical components of Active Directory include domain controllers, global catalog servers, and data store. Domain controllers are the primary servers in Active Directory and are responsible for managing authentication, authorization, and other functions. Global catalog servers are domain controllers that maintain a subset of Active Directory data for the entire forest. The Active Directory data store is a centralized database that contains all the information about the resources, users, and computers in the Active Directory environment. It stores information such as user account information, group policy settings, and other configuration data. The data store is typically stored on a Microsoft Windows domain controller and usually replicated to other domain controllers in the environment for redundancy and reliability.

Four common attacks that have been identified as major threats to AD environments are LLMNR(Link-Local Multicast Name Resolution) poisoning, SMB relay, Pass the Hash, and Token Impersonation. LLMNR poisoning is an attack that redirects network traffic by spoofing response to a LLMNR (Link-Local Multicast Name Resolution) query. SMB relay is a technique used to capture user credentials by relaying SMB (Server Message Block) authentication requests from a vulnerable client to another system. Pass the Hash is an attack that allows an attacker to use a captured password hash to authenticate to a remote system without cracking the password. Token Impersonation is an attack that involves copying a security token from one process to another, allowing the attacker to gain access to resources as if they were the original user.

Implementation

The research was aimed at building a virtual Active Directory network that would be used to conduct the penetration testing. This was actualized by setting up domain controllers, client computers, and other network resources, and penetration test was conducted on the Active directory set up. This involved using various tools and techniques to simulate different attacks, including LLMNR poisoning, SMB relay, pass the hash, and token impersonation.

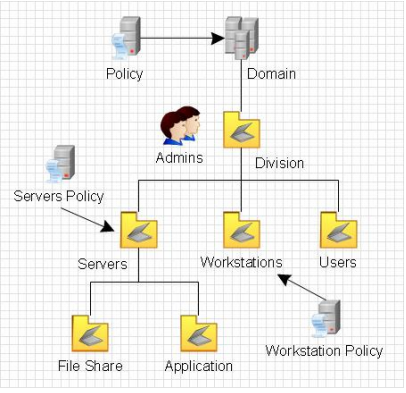

Fig 1 Simple Active Directory Architecture

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue IV, April 2024

The data collected from the penetration tests was then analyzed using various methods, including statistical analysis and visualization techniques.

This data was used to compare the different penetration testing paradigms.

Minimum hardware requirement for the research is 60gb Disk Space and 16GB of RAM, the components that is used includes Virtual Machine, Windows Server, Windows Enterprise and Kali Machine for Attacking the Active Directory Network.

A. Result

The Four Attack Vectors were compare dusing Seven Criteria namely, Process, Impact, Difficulty, Detection, Required tools, Complexity, and Susceptibility to defense mechanisms as presented in Table 1.

Figures 2 and 3 presents the graphical representation of criteria based on its intensity, The Value of 1 indicates the simplest attack while a value of 4 indicates the most complex.

Table 1 Comparison Using Selected Criteria

Criteria	LLMNR Poisoning	SMB Relay	Pass the Hash	Token Impersonation
Process	Involves intercepting and redirecting network traffic by exploiting a weakness	Involves relaying SMB authentication requests to other systems on the network	Involves stealing and using a password hash to authenticate as another user on the network	Token impersonation involves stealing and using a security token to impersonate another user on the network
Impact	Allows an attacker to intercept and redirect network traffic, potentially gaining access to sensitive information	Allows an attacker to gain unauthorized access to network resources	Allows an attacker to authenticate as another user on the network, potentially gaining access to sensitive information or systems	Allows an attacker to impersonate another user on the network, potentially gaining access to sensitive information or systems.
Difficulty	Relatively easy to carry out	More complex and require a higher level of technical skill to carry out successfully.	More complex and require a higher level of technical skill to carry out successfully.	More complex and require a higher level of technical skill to carry out successfully.
Detection	Difficult to detect, as the attacker is redirecting network traffic rather than modifying or altering it	More easily detected, as they involve changes to the authentication process or the use of stolen credentials.	More easily detected, as they involve changes to the authentication process or the use of stolen credentials.	More easily detected, as they involve changes to the authentication process or the use of stolen credentials.
Required Tools	Requires specialized software or a tool such as Responder, Metasploit	Requires tools such as Metasploit, Impacket, NTLMRelayX	Requires tools such as Crackmapexec, PsExec, SecretDump	Requires tool called Incognito
Complexity	Less Complex to carry out than SMB Relay	More Complex to carry out than LLMNR Poisoning	Less Complex to carry out than Token Impersonation	More Complex to carry out than Pass the Hash
Defense Mechanism	More susceptible to network segmentation or firewall rules	More susceptible to network access controls or multi-factor authentication	More susceptible to password policies or security awareness training	More susceptible to proper access controls and permissions management.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue IV, April 2024

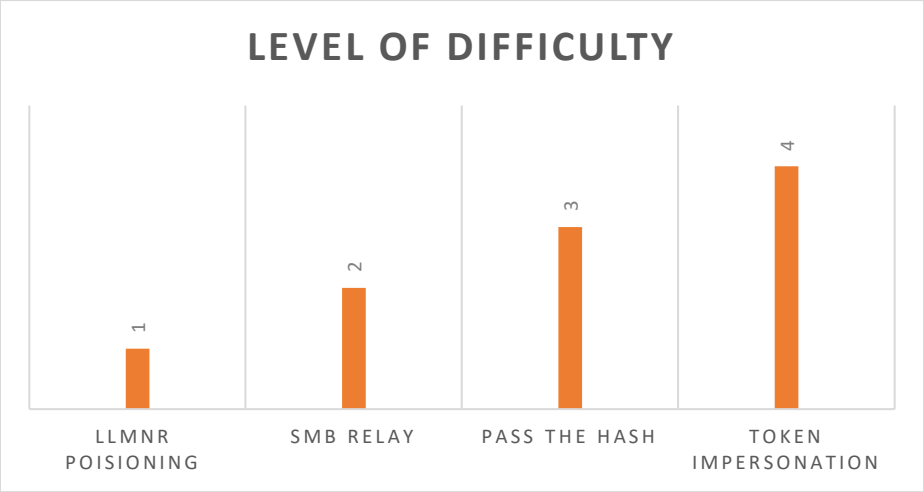

Fig 2: Criteria 1 -Difficulty

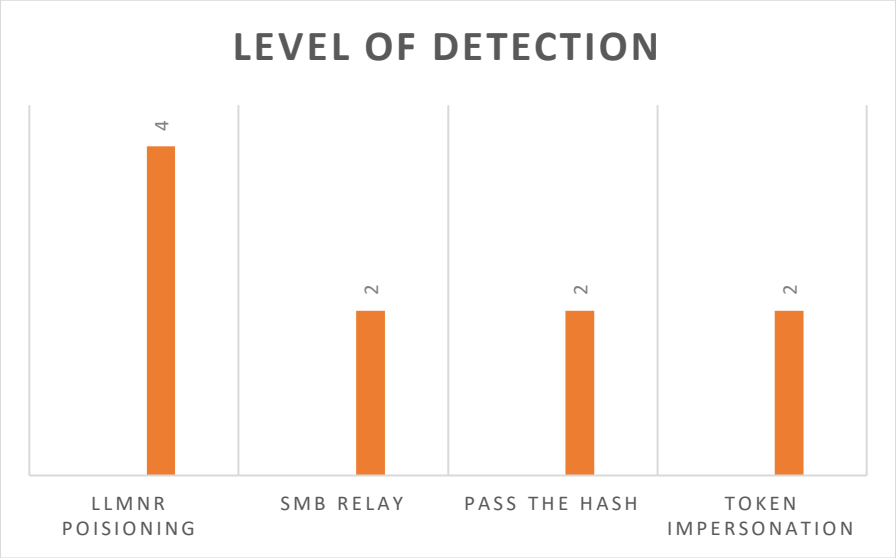

Fig 3: Criteria 2 - Detection.

Note: level of detection for each of these attacks can vary depending on the specific implementation of the target environment.

Conclusion

Active Directory is a critical component of many organizations' IT infrastructure and it is important to secure it against potential attacks. Active Directory attacks can take many forms, including privilege escalation, lateral movement, and data exfiltration. Some common methods used in Active Directory attacks include Pass the Hash, Token Impersonation, LLMNR Poisoning, and SMB Relay. To prevent Active Directory attacks, organizations should implement a robust security program that includes regularly patching systems, using strong passwords and multifactor authentication, monitoring network activity for suspicious activity, and training employees on how to identify and avoid phishing attacks. Additionally, organizations should consider implementing security tools and techniques such as network segmentation, privilege access management, and intrusion detection systems to help detect and respond to Active Directory attacks. In conclusion, securing Active Directory against potential attacks is crucial to the security and stability of an organization's IT infrastructure. By implementing a comprehensive security program and staying informed about the latest threats, organizations can minimize the risk of Active Directory attacks and ensure the continued protection of their sensitive information.

References

1. Active-directory-penetration-testing: redteamslabs.in. (2021, December 20). Retrieved from redteamlabs.in: https://redteamlabs.in/
2. Adam, B. (2019). bloodhound-active-directory-domain-admin.aspx. Retrieved from mcpmag.com: https://mcpmag.com/articles/2019/11/13/bloodhound-active-directory-domain-admin.aspx
3. Bhardwaj, R. (2022). Active Directory Forest. Retrieved from ipwithease: https://ipwithease.com/
4. Bhardwaj, R. (2022). WHAT IS AN ACTIVE DIRECTORY TREE? Retrieved from ipwithease: https://ipwithease.com/
5. Chai, W. (2022). Active-Directory. Retrieved from TechTarget: https://www.techtarget.com/

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue IV, April 2024

6. DCtheGeek, M., & Msatranjr. (2020). Forest. Retrieved from Microsoft: https://docs.microsoft.com/
7. Doubleoctopus. (2022). threats-and-tools/golden-ticket/. Retrieved from doubleoctopus.com/security-wiki: https://doubleoctopus.com/security-wiki/threats-and-tools/golden-ticket/
8. Dr. Shwetav Sharad, A. S. (2019). Research Paper on Active Directory. International Research Journal of Engineering and Technology (IRJET), 1-2.
9. Imperva. (2021). Penetration Testing. Retrieved from Imperva: https://www.imperva.com/learn/application-security/penetration-testing/
10. Kali. (2022). Retrieved from https://www.kali.org/: https://www.kali.org/
11. Khari, M., & Bajaj, C. (2014). Motivation For Security Testing. Global Research in Computer Sciences, 27.
12. Komal, M. (2018). Network Security Implementation using Penetration Testing. International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES), 1-6.
13. Microsoft. (2014). Microsoft. Retrieved from Microsoft: https://docs.microsoft.com/
14. msatranjr. (2019). Domain Trees. Retrieved from Microsoft: https://docs.microsoft.com/
15. pass-the-hash-pth-attack. (2022). Retrieved from hwww.beyondtrust.com: https://www.beyondtrust.com/resources/glossary/pass-the-hash-pth-attack
16. Raj, C. (2021). active-directory-enumeration-powerview. Retrieved from www.hackingarticles.in: https://www.hackingarticles.in/active-directory-enumeration-powerview/
17. resources: tracesecurity. (2021). Retrieved from tracesecurity: https://www.tracesecurity.com
18. Rubenstein, B. (2012). Active Directory domain (AD domain). Retrieved from techtarget: https://www.techtarget.com/
19. Securitytutorials. (2022). token-impersonation-attack. Retrieved from securitytutorials.co.uk: https://securitytutorials.co.uk/token-impersonation-attack/
20. Skoudis, E. (2008). Planning, scoping and recon. Proceedings of the Network penetration, 12.
21. Svidergol, B. (2017). Active Directory Database. Retrieved from Netwrix Blog: https://blog.netwrix.com/
22. Techopedia. (2020). domain-controller-dc. Retrieved from domain-controller-dc: https://www.techopedia.com/
23. Trace Security. (2021). Mitigating IT Security Risks with Penetration Tests. Retrieved from Tracesecurity: https://www.tracesecurity.com/resources/whitepapers/mitigating-it-security-risks-with-penetration-tests
24. University, T. T. (2019). About organizational units in Active Directory. Retrieved from University Information Technology Services: https://kb.iu.edu/
25. Venu, S. (2022). kerberoasting. Retrieved from www.crowdstrike.com: https://www.crowdstrike.com/cybersecurity-101/kerberoasting/
26. Vladimir, U. (2020). heimdalsecurity.com. Retrieved from heimdalsecurity.com: https://heimdalsecurity.com/blog/what-is-an-smb-relay-attack/
27. Wikipedia. (2022). Kali_Linux. Retrieved from https://en.wikipedia.org: https://en.wikipedia.org/wiki/Kali_Linux