Active Directory: A Defensive Service

CYSE 280: Research Paper

Kevin Durand, kdura002

Table of Contents

I. Introduction

In modern times it is more important than ever to have well made, secure computer systems, this becomes especially important for servers hosting multiple other servers or computers. On a windows server, one of the tools that you can use for this defense is what is known as Active Directory control. Active directory, hereby referred to as AD, can best be described as the executive leader of a server group; by administering the server, this service is able to control and defend their related local network. By comparing AD responses to some of the steps cyber attacks and malicious software use when exploiting a system. AD creates a web of computers or servers that it administers, in this web different computers are distinct from each other and the servers that are above them, this distinction allows for a good defense against the Reconnaissance step in a cyber attack. With the ability to administer password and secondary authentication, the AD is capable of creating a strong defense against intrusion Another step in the cyber attack list that is well defended against is Lateral Movement into the system; with a good understanding of best practices, a Cyber Security minded person is able to isolate those systems from others. Properly administering, an AD can be used as ablative armor against cyber attacks, and keeps a Microsoft system secure.

II. AD Services

AD, Active Directory is an administrative set of services and set ups that allow for multiple computers and users to all be connected and managed under one unifying service. The first thing to detail is the structure of the AD, it was mentioned before that this is similar to a web of interconnected computers, users, and groups; the better way to describe the inhabitants of the web and the owner of the web, as trees overlooked by a single forest, the trees are called the domain of the the forest. In this ecology based themology each tree represents a group of users, servers, and/or computers; but it

can also mean a group/tree of any of those set up to interact with the system in specific ways. The Forest is actually a number of different elements that work together, while using the AD, to administer over that entire forest, be it a single entity or a single group of entities. One of the biggest uses of the Active Directory is in its ability to grant or remove access to different levels of control of the entire forest to different domains or trees, based on department criteria. Quest, a company the oversees cyber security software, has this to say about domains "..a domain is a management boundary.." (Quest) meaning that domains are about the actual manageable pieces of an AD, its main purpose is to make sure all shared groups have a defined role and place to be. The Forest of an AD is the part that matters the most for security, the forest represents the separation of access and control between different trees or domains, "..A forest is a security boundary.." (Quest). Focusing more on the Forest side of the AD, i.e. the security side; any given company has a number of different levels of access and control granted to the trees, this separation of domains allow no one single element of the forest to be able to grant access to the entire forest, or even other trees in different parts of the forest. The Forest creates a local network that all of the trees are connected to, a server with multiple pcs and users; and the access to that network, communication between all domains and trees is how the system is administered defensively. With the management of domains put into proper working groups, distinct of other groups by purpose or access, and the security potential of the forest, to keep control and limit access of the trees of that service; the AD is able securely manage any large network.

III. Steps of a Cyber Attack

With the rise of computers, servers, and the internet, there are no end to the number of malicious actors or software seeking to break into any computer network. Generally when an attack is carried out against an exploit, it does so with a number of different steps; each step in the attack cycle represents a distinct defining moment in the attack itself. The first step, known as "Reconnaissance" (Morano) , for an attack to have any level of success information needs to be learned about the system; these information seeking actions can be anything from social engineering to taking a password or learning the mac addresses of certain physical entities in the network. The next step in the attack will be the "Planning" (Morano) stage of the attack; now that the attacker has the information that they need about the system they use software or social engineering to gain access to the system. The attacker has their program all ready to go, now they need to actually get it into the system, the "Intrusion" (Morano) step of the cyber attack will get their software into a part of the system that it can start doing whatever task it needs to complete, based upon the results of the "Planning" phase (M,j). Now that the software is in the system, following the "Intrusion" (M,j) phase, it needs to propagate and move about the system, which is completed with the combination of two ways; the malicious software moves laterally about the system, between two computers of the same tree or administrative access, or it moves up in the system, by accessing systems that give it higher levels of administrative access. The last phase of the attack, now that the attacker has access to that system, does whatever it came to do, and removes any trace of itself. The step of the attack is very specific to AD systems, known as "Exfiltration and cleanup" (Morano), generally at this point the attacker is trying to put ransomware on the computer, in an attempt to force the owner of the system to want to pay money to get that back.

IV. Reconnaissance

When reconnaissance is carried out by an cyber attacker, against a computer system, the attacker is generally looking for two very important pieces of information, are the digital assets of a company big enough to warrant the effort to break into the system, and what is the layout of the computers in the system that are trying to be attacked. Blumira, a cyber security company gives a concise run down of this phase of a cyber attack, "reconnaissance is the practice of covertly discovering and collecting information about a system..". In terms of an AD, what an attacker needs to know about the system is the physical mac and IP address of machines in its forest and how those different machines are connected. Ideally this phase would also assess how easily the system could be broken into. The way that a Forest of an AD is capable of defending against this level of attack, would be through the natural obscuring of machine identities and addresses by the very nature of the Tree itself. The Domains that form to make the trees are generally connected to an internal router, overseen by a computer or server, along with whatever server oversees that next level of abstraction. Let's say that an attacker tries to gain information on the attacker by phishing the password of an employee, if an AD is administered correctly, gaining access to that employee's computer is overall very useful; implemented correctly, it would take a lot more work for the intruder to try and figure out exactly how the system is laid out, or even in what direction they need go to hack the infrastructure.

[this space left intentionally blank]

V. Intrusion

It is possible, through either poor management of the local network, or from unseen bugs in the system, that a computer system has been successfully inspected, assessing the quality of the information and the structure of the system. At this point the attacker has not yet truly gotten their software onto the system, so they would now try more concentrated efforts to get that malicious software somewhere where it could actually break into the system. Another aspect of the AD is its ability to keep tabs on all operations carried out in its forest. Oversight, one of the passive features of a properly managed AD, allows people with high enough access to view the interactions between computers on a system, the software on that computer, and the data connection that computer has with the network. The Forest also has the ability to administrate the systems under it, since the AD is at the top of the Forest, it has the ability to pass software and scripting changes to the computers under. One of the main techniques of a software trying to gain access with your systems, is to give that software the identity of legitimate software that mimics an existing service. One of the worst kinds of trojans will show up as a duplicate, or replace a current Windows process, think System 32/64 configuration files; replacing the configuration files bricks windows, while A script can be devised, affecting every single tree in the AD from the top level, that looks for the generation of new or old processes and stops those processes for review. After the security professional investigates the new processes it can confirm or deny the changes.

VI. Lateral Movement and Privilege escalation

After the software has found its way into the system, it needs to move to vital portions of the system or gain higher levels of privilege. Gaining access to a vital portion of the forest means that the malicious attacker and/or program have managed to get to the information they wish to ransomware. Sometimes; either because the files that are wanted for the ransomware are at a higher level in the

administrative structure of the forest or because the attacker is trying to gain administrative control over the entire AD; the attacker seeks to gain administrative rights, either to give the program power and control over the system. In the AD system, however, there is a mechanism that involves the level of privileges between different layers of the system. In the public library at Old Dominion University, almost anyone can access and interact with the computers; all you would need to access is a students' username, password, and access to their two factor system. In the AD system this computer is low on the list of privileges and an attacker would have a hard time getting into other computers or systems with higher administrative rights. At the same time, the ITS team at ODU has computers, that with the right logon and authentication information you would gain access to the entire system. The level of computer with that kind of access would be in a physical location not easily accessed, and be obscured from lower level computers.

VII. Conclusion

Active Directory, AD, sitting at the top of a Forest of Trees of Domains; is able to be effective armor against cyber attacks; deterring a number of the phases a cyber attack requires to succeed. The Active Directory itself is a web or forest of computers, all administered by a small team of IT security, that both manages and protects the numerous computers and users on the network. Using five different steps or phases malicious software makes its way into a computer system, with the intent to control the system, encrypt and ransom the information on the system, or brick the system itself. Leveraging the lack of attachment amount Trees in the AD Forest, the AD is able to protect itself from invasive informational hacks. With the right control and scripting an AD is capable of defending itself against intrusions, with an emphasis on catching malicious software acting as important processes. In a number of different ways the Active Directory of a Windows server system is ablative

armor in the fight against malicious software and actors, and performs an important security task on the system.

References

1. *What is Active Directory? Learn what AD is and how it works.* (2022). Quest, Blog. https://www.quest.com/solutions/active-directory/what-is-active-directory.aspx
2. Morano, J. (26, Sept. 2022) *The anatomy of Active Directory Attacks.* Quest, Blog. https://blog.quest.com/the-anatomy-of-active-directory-attacks/
3. Maor, T. (17 April, 2019) *LDAP Reconnaissance - the foundation of Active Directory attacks.* Microsoft, Tech Community https://techcommunity.microsoft.com/t5/security-compliance-and-identity/ldap-reconnaissance-the-foundation-of-active-directory-attacks/ba-p/462973
4. Terra, J. (29 Nov, 2022) *Top 35+ Cybersecurity Terms You Need to Know.* Simplilearn. https://www.simplilearn.com/top-cybersecurity-terms-you-need-to-know-article
5. *What Is a Trojan Horse Virus?* (Visited 15 Oct. 2022) Fortinet. https://www.fortinet.com/resources/cyberglossary/trojan-horse-virus
6. Chapter 4: Introduction to Active Directory and Account Management: User Account Management.