Implementing and Evaluating an Automated Active Directory Vulnerability Identification, Exploitation, & Reporting Tool

Thomas G. Gardner 1800028
School of Design and Informatics
Abertay University
DUNDEE, DD1 1HG, UK

Abstract

Context:
Vitally important in the day-to-day operations of modern businesses, Active Directories (AD) administers authentication and authorisation for the organisation. As such, ADs are often the main instrument used by attackers to extract sensitive information and disrupt the day-to-day operations of a company. Despite numerous patches and security guidance, attacks are still commonplace. Lengthy audits of ADs can often miss dangerous misconfigurations and vulnerabilities which could lead to total takeover of the victim's organisation.

Aim:
The aim of this project is to develop an intuitive tool that exploits vulnerabilities in an Active Directory then automates the report writing process.

Method:
A comprehensive review of relevant academic literature will be carried out first in order to investigate the most common practices used in the industry, the most critical AD vulnerabilities, and to devise the most efficient approach when development of the project. With information obtained from relevant literature, a prototype tool will be designed and developed with Python to identify, exploit, and report vulnerabilities affecting AD.

Results:
The developed tool will be tested against randomised active directories in order to generate a large quantity of vulnerability reports. These results will then be analysed and evaluated in detail to discover patterns and to see how many critical vulnerabilities the tool exploited.

Conclusion: This project will result in the creation of an automated tool that attacks and reports common vulnerabilities affecting AD. The information obtained should mitigate the impact of attacks against individuals and companies.

Keywords: Active Directory, AD, Domains, Post Exploitation, Persistence, Kerberos, Pass-the-Hash, Pass-the-Ticket, Man in the Middle, Authentication, Credentials.

1. Introduction

In the modern world, individuals and companies are looking for more efficient and straightforward ways to control and monitor thousands of users and computers within their networks. Arguably, the most important and most widely used service to achieve this requirement is Microsoft Active Directory (AD), first introduced with Windows Server 2000.

In short, Active Directory is a database and set of services used by companies and large enterprises worldwide to store usernames, computers, and other sensitive information. Active Directory is also used as their primary method for authentication. Companies are not the only sectors to use Active Directory. The service is also regularly used and highly essential in the education sector as well. Active Directory allows Schools and Universities to separate departments, staff, faculty, and students into their subdomains and groups, which means IT staff can control and monitor what resources each account and group has access to and privileges. Active Directory also allows campuses to have a central repository of all accounts for services like centralized email access, access to lab machines in classrooms (Spigelmyer & Hron, 2019). However, when there is a service as essential and widespread as Active Directory, there are always going to be external parties looking to exploit it.

Approximately 90% of Fortune 1000 companies worldwide use Active Directory, so unsurprisingly, they are prime targets for attackers looking to extract sensitive data and information from a company. Attacks against Active Directory are so common; recent estimates show that around 95 million accounts are targeted by hackers every day, and this number will inevitably increase as the world becomes more and more interconnected. Another alarming discovery was found by a group called Semperis. In 2020, the group surveyed thousands of companies around the world, and they found out that 97% of organisations said that Active Directory is critical to the daily operations of their company (businesswire, 2020). However, more than half of this number had never actually tested their Active Directory cyber disaster recovery process or did not have a disaster plan in place at all.

Since the Active Directory attack surface is so vast there are many different paths hackers can use to gain access to domain administrator accounts. The typical strategy hackers use is to first gain a foothold in the network, then elevate privileges with post exploitation attacks until domain admin access is achieved. However, this process is time-consuming as there are wide variety of complicated attacks and tools that need to be used in order to achieve admin access. An example of the Active Directory kill chain can be seen in Figure 1 below.

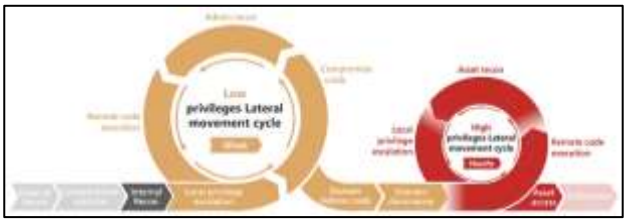

Figure 1: Active Directory Kill Chain

In order to address the problem in the introduction, this project aims to develop an intuitive tool that identifies and exploits vulnerabilities in an Active Directory then automates the report writing process. The main focus for the project is to address the problem put forward in the following research question:

Can an automated tool effectively mitigate risks to clients by reporting potential vulnerabilities in a detailed, yet intelligible manner so non-technical users can understand?

In order to satisfy the project aim, the following objectives will be fulfilled. The first objective is to perform a search for academic papers or authoritative sources, and from this relevant literature, review the most effective practices experts use to attack and defend Active Directory environments. With information and conclusions obtained through the literature review, the second objective is to design an Active Directory exploit and report writing tool. The third objective is to implement the Active Directory exploit and report writing tool once the design phase has been finalised. Finally, with the implementation stage completed, the fourth objective is to examine, and commentate on the results and the effectiveness of the tool.

The remainder of this proposal will continue as follows: Starting with the background, this section will conduct a critical review of relevant material, using academic and technical sources. These references will then inform a Methodology, including a description of the testing and validation methods, in the following section. Finally, concluding with a summary of the project's significance and how the subject field will significantly benefit from its contribution.

2. Background

2.1 Active Directory Vulnerabilities

As is established from an abundance of academic research, Active Directory is a complex and expansive service used by millions of individuals and companies worldwide. Unfortunately, most domain administrators have a limited grasp of network security. Therefore, as a consequence, there are now a considerable number of vulnerabilities affecting Active Directory.

Initial attack vectors are attacks targeting vulnerabilities that give a hacker an initial foothold in the domain. These attacks commonly target the so-called 'low hanging fruit' vulnerabilities that are relatively easy for an attacker to discover and exploit. According to an academic paper published in 2020, some techniques attackers use to gain access into an Active Directory are through attacking AD credentials. These attacks would involve an attacker using techniques such as requesting sensitive data such as AD accounts and passwords through Dcsync attacks, Brute forcing AD account login forms, or detecting user or admin credentials with keylogging software (Bohte & Offerman, 2020).

The Man in the Middle Attack (MitM) is another vector attackers can use to gain an initial foothold in an Active Directory. A relatively recent academic paper on MitM attacks explains that attacks such ARP Spoofing, DHCP spoofing, DNS spoofing, and IP spoofing can be used to intercept legitimate communication between hots and control the transfer of sensitive information. While this is occurring, the hosts will be unaware of the middleman (Conti, et al., 2016). In the context of Active Directory, this attack could be used to capture user or admin credentials passing over the network, then using a technique like Pass the Hash to gain a foothold into the domain.

2.2 Active Directory Post Exploitation

Once a foothold has been gained into an Active Directory, the next step is to elevate to domain administrator privileges. In order to obtain admin privileges, post-exploitation attacks will need to be used against regular user accounts in the domain. There is a wide selection of documented attacks that can be used against a domain. The Kerberoast attack is a widespread and well- documented attack. This attack exploits a flaw in Kerberos, which is a Microsoft authentication protocol. An ICISSP conference paper describes this attack as an exploit which enables an attacker to crack passwords for remote service accounts offline (Kotlava, et al., 2020). The paper goes on to say that this attack requires a foothold in the domain because a TGT ticket has to be requested from the domain controller as an authenticated AD user. The stolen ticket can then be cracked offline.

Another academic paper published in discussed several Active Directory post-exploitation attacks. The attacks mentioned taking advantage of hashes and tickets stored in local client machine memory. The attack 'Pass-the-hash' is an attack that is used once a hacker has compromised a domain client machine. The attacker then harvests password hashes stored in LSA memory and then re-presents these hashes to impersonate their corresponding user accounts. The next attack mentioned is 'Pass-the-Ticket'. This attack requires a hacker acquiring Kerberos tickets cached in LSA memory and using this to gain access to other resources in the domain. This attack is useful as an attacker can acquire a TGT ticket, a TGS ticket of a domain user, or a KRBTGT hash on a domain controller (Nichols, et al., 2016). The latter attack is powerful as it allows an attacker to create unlimited tickets, which grants them unlimited access to the Active Directory. The paper goes on to explain that these attacks are simple because hackers can use readily available tools such as Mimikatz, Windows Credential Editor and Metasploit.

2.3 Vulnerability Report Writing

When generating AD vulnerability assessment reports, it is vitally important to present the business risk to a client in a transferable and digestible way while also keeping the report detailed. To achieve this, the tool will produce findings in line with the vulnerability reporting guidelines detailed in ISO29147 This document provides requirements and recommendations to vendors on the disclosure of vulnerabilities in products and services (ISO, 2018). The document also provides guidelines on receiving reports about potential vulnerabilities; guidelines on disclosing vulnerability countermeasures; an overview of vulnerability disclosure concepts; and techniques and policy considerations for vulnerability disclosures (ISO, 2018).

3 Method

3.1 Research

The first stage of the project will be the research phase which will commence with a comprehensive literature review of relevant academic and technical sources. These sources can consist of academic papers, journals, blogs, and other online authoritative sources relating to Active Directory. The overall purpose of this stage is to investigate the most common security practices used in the industry, to acquire a greater understanding of the most critical vulnerabilities affecting Active Directory, and to work out how the AD attacks can be scripted. Performing this phase to a high standard will ensure the prototype tool attack and report the most critical security vulnerabilities.

3.2 Development

With the research phase completed, the next step is to begin developing a design of the prototype tool. In order to test the feasibility of the project, a demo will be carried out under strict supervision. Furthermore, this demo will be helpful to iron out any serious issues early in the development process.

The implementation phase of the project will start once the design of the tool has been finalised. The prototype tool will be developed using the Python programming language as it is the syntax is simple, it is well documented, and it has a large number of useful built-in libraries. These factors should increase the development speed. The prototype tool will attempt to identify the low-hanging fruit vulnerabilities affecting an Active Directory, and it will then try to exploit these vulnerabilities using a number of readily available tools. The prototype tool will be most efficient when used in tandem with Bloodhound, developed by Andrew Robbins, Rohan Vazarkar, and Will Schroeder. Bloodhound is an intuitive tool that displays the relationships of users and computers in a domain, and the shortest attack paths to domain admins. This tool utilises graph theory to automatically generate a map of a target domain, significantly increasing the speed of an attack. A screenshot of what a user sees when using Bloodhound can be seen in Figure 2 below.

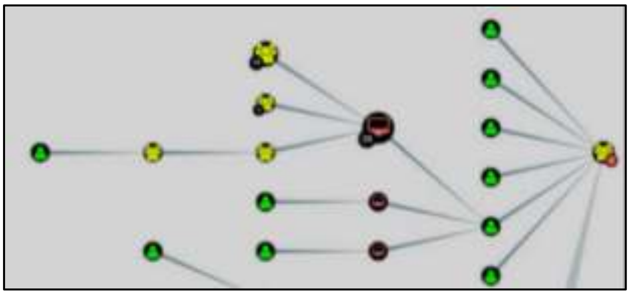

Figure 2: Shortest Paths to Domain Admin

The tool will move onto the reporting stage once the identification and exploitation stage has been completed. The tool should reduce the time it takes to report vulnerabilities back to a client by automatically generating Active Directory vulnerability. The standards set out by ISO29147 will need to be followed in order to make the vulnerability reports as detailed, formal, and comprehensive as possible (ISO, 2018). Overall, the tool will be developed using the prototyping methodology as this will be the most efficient way of completing the project with one person.

3.3 Evaluation

The testing phase will commence once all the intended features of the tool have been implemented. The developed tool will then be tested in order to evaluate the effectiveness, performance, and capabilities of the tool. An ideal test environment will be testing the tool against several randomized Active Directories since this will generate a greater quantity of vulnerability reports. Once all the reports have been obtained, they will need to be evaluated in detail. This will be carried out in order to examine if the tool successfully identified and exploited the most critical Active Directory vulnerabilities. This stage is also an opportunity to get the reports reviewed by other individuals, which is essential since it tests if the reports are detailed yet straightforward enough for individuals to understand.

4 Summary

By fulfilling the project objectives and addressing the research question, the overall outcome of the project will be a python based Active Directory vulnerability detection and exploit tool. This tool will allow users to test the security measures of their own domain, which should help in reducing the severity of Active Directory attacks in the future. The tool will also script the report writing process using ISO guidelines, so a shorter time is spent manually writing penetration test reports. Furthermore, it is hoped that this project will result in a one-of-a-kind tool that could improve auditing and be a helpful addition to an ethical hacker's penetration testing toolkit.

References

Bohte, E. & Offerman, N., 2020. *Analysis of Bypassing Detection by Microsoft Advanced Threat Analysis.* [Online]
Available at:
https://www.semanticscholar.org/paper/Analysis-of-Bypassing-Detection-by-Microsoft-Threat-Bohte-Offerman/cc94811a77d017a20451d91dd787262d821fb8f0
[Accessed 9 October 2021].

businesswire, 2020. *84% Of Organizations Report That the Impact of an Active Directory Outage Would Be Significant, Severe, or Catastrophic in the Latest Semperis Study.* [Online]
Available at:
https://www.businesswire.com/news/home/20200824005110/en/84-Of-Organizations-Report-That-the-Impact-of-an-Active-Directory-Outage-Would-Be-Significant-Severe-or-Catastrophic-in-the-Latest-Semperis-Study
[Accessed 14 October 2021].

Conti, M., Dragoni, N. & Lesyk, V., 2016. *Survey of Man In The Middle Attacks. IEEE Communications Surveys & Tutorials.* [Online]
Available at: https://www.semanticscholar.org/paper/A-Survey-of-Man-In-The-Middle-Attacks-Conti-Dragoni/4c7dc21ac9155bec100b33da601b04c31c4de834
[Accessed 9 October 2021].

ISO, 2018. *ISO/ IEC 29147:2018.* [Online]
Available at: https://www.iso.org/standard/72311.html
[Accessed 14 October 2021].

Kotlava, L., Buchovecka, S. & Lorencz, R., 2020. *Active Directory Kerberoasting Attack: Monitoring and Detection Techniques.* [Online]
Available at:
https://www.insticc.org/node/TechnicalProgram/icissp/2020/presentationDetails/89550
[Accessed 10 October 2021].

Nichols, J., Taylor, B. & Curtis, L., 2016. *Security Resilience. Proceedings of the 11th Annual Cyber and Information Security Research Conference.* [Online]
Available at:
https://dl.acm.org/doi/10.1145/2897795.2897800
[Accessed 11 October 2021].

R, N., 2021. *Active Directory Kill Chain Attack & Defense.* [Online]
Available at: https://github.com/infosecn1nja/AD-Attack-Defense/blob/master/README.md
[Accessed 14 October 2021].

Spigelmyer, A. & Hron, D., 2019. *Re-Planting All Your Trees in One Forest: Deploying an Enterprise-Wide Active Directory at Penn State.* [Online]
Available at:
https://dl.acm.org/doi/fullHtml/10.1145/3347709.3347781
[Accessed 7 October 2021].