ACTIVE DIRECTORY ATTACK PATH REMEDIATION USING BLOODHOUND

Department of Computer Science, Stephen F. Austin State University

Adam Percell - adam.percell@sfasu.edu
Faculty Mentor: Dr. Christopher Ivancic – ivanciccp@sfasu.edu

ABSTRACT

This project uses Bloodhound to analyze a live Active Directory domain, compiling the findings into four categories:

1. Cross-tier contamination (tier zero credentials being used on lower tier systems, or vice versa)
2. Default permissions (large groups of accounts granted administrative rights by default)
3. Excessive privileges (non tier zero accounts having control over tier zero objects)
4. Kerberos issues (exploits within the Kerberos authentication system such as “kerberoasting” and Kerberos delegation)

These categories represent attack paths that can all be exploited by an attacker to gain total control over the domain, and can be remediated by maintaining more careful control over tier zero permissions and access.

INTRODUCTION

Much effort and study in cyber security is focused on preventing unauthorized access to an organization’s environment, but once an attacker has gained access, what can they do? What attack paths are open to them, and how much damage can they cause? Bloodhound is an application that aims to help security professionals answer these questions about their own environment. Many organizations use Microsoft Active Directory (AD) to manage the digital structure of their organization; this project analyzes the AD domain of one organization using Bloodhound to enumerate the various attack paths, then demonstrates the exploitation and remediation of those vulnerabilities in an offline test environment set up to mimic the identified attack paths. In this project, 4 broad categories of attack paths are discussed, each of which expose tier 0 objects to attackers in some way.

RESEARCH OBJECTIVE

The goal of this project is to explore attack paths that can arise within an active directory environment, to understand how a successful penetration attempt can allow an attacker to gain full control over a domain. This study does not include methods of gaining initial access to an environment, instead focusing on what avenues of exploitation may be available after gaining access.

ACTIVE DIRECTORY SECURITY

Microsoft provides the following 3 “commandments” of the AD tier model, [1]:

1. Credentials from a higher-privileged tier must not be exposed to lower-tier systems.
2. Lower-tier credentials can use services provided by higher tiers, but not the other way around.
3. Any system or user account that can manage a higher tier is also a member of that tier, whether originally intended or not.

The attack paths found by bloodhound have to do with gaining control over tier 0 objects. Tier 0 objects are the highest level of privilege in the domain: accounts and devices which have administrative control over the entire environment through the ability to manage identity and permissions enterprise-wide [1].

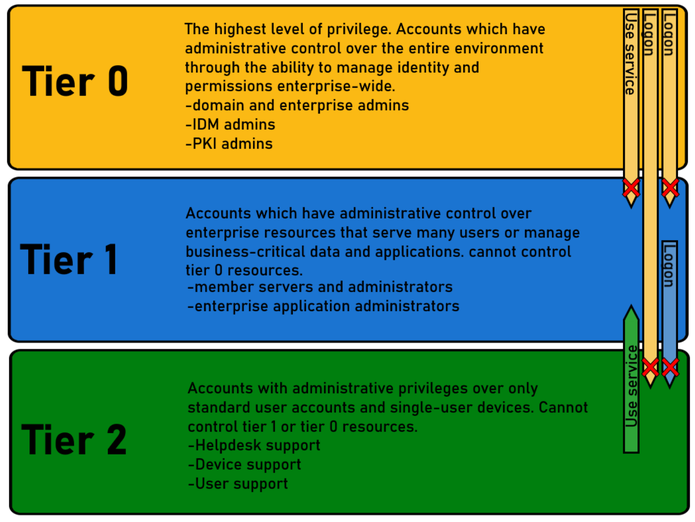

Figure 1. Tiers of privilege in an AD environment (edited) [1]

STAGE 1: ENUMERATION

Cross-Tier Contamination

-In this project, cross-tier contamination refers to any case where tier zero credentials are exposed to a lower tier, or when lower tier accounts have access to higher tier devices.
-In the domain analyzed here, Bloodhound identified tier zero users who had used their credentials to sign in to lower tier devices, as well as non tier zero users with permission to remotely execute code on tier zero devices, using Microsoft’s DCOM framework.

Default Permissions

-Default permissions refers to large groups of users given powerful permissions over devices by default, rather than being granted only when needed.
-Bloodhound identified large default groups with remote desktop (RDP) access, as well as local administrative rights.

Stage 1: Enumeration – continued

Excessive Privileges

-Excessive privileges in this context refers to a non tier zero object which has privileges over a tier zero object.
-In this case, Bloodhound found users with generic-all, ownership, and DCsync privileges on tier zero machines, as well as a non tier zero server hosting a certificate authority.

Kerberos Issues

-Kerberos is an authentication method within Active Directory, this category refers to attack paths which would allow an attacker to bypass or exploit Kerberos.
-In this environment, Bloodhound noted accounts that could be vulnerable to a specific attack called kerberoasting, as well as tier zero accounts vulnerable to Kerberos delegation attacks.

STAGE 2: EXPLOITATION

Cross-Tier Contamination

-To exploit a cross-tier contamination vulnerability, an attacker will need to use non tier zero credentials to gain access to tier zero objects.
-On a non tier zero PC in the domain, a domain admin had signed in with their password. Using various free tools, an attacker can brute force the domain admin’s password offline in order to impersonate them, or target a user with DCOM privileges to execute malicious code on a tier zero device, despite not having access to a tier zero password.

Default Permissions

-Default permissions issues can be exploited by gaining access to any account in the group which has the permissions, at which point the attacker has more access than they should (either administrative rights or RDP).

Excessive Privileges

-To exploit an excessive privileges vulnerability, an attacker just needs to find the user or device with these privileges.
-Certain user accounts in this domain had generic-all privileges on tier zero machines, others had ownership of tier zero machines, and others had DCSync privileges, which allows an attacker to access users’ passwords.

Kerberos Issues

-Kerberos issues are exploited in a few ways, but the two listed here both rely on intercepting parts of the Kerberos authentication process, by having access to one of the devices involved.

STAGE 3: REMEDIATION

Cross-Tier Contamination

-To fix cross-tier contamination issues, it is critical to ensure that the tiers do not mix, meaning tier zero accounts are only exposed to tier zero devices, and vice versa.

Stage 3: Remediation – continued

Default Permissions

-Resolving default permissions issues are simple: only grant powerful privileges like local admin rights or RDP access to specific, limited groups, or individual users.

Excessive Privileges

-Remediation of this category is very similar to cross-tier contamination: ensure that only tier zero objects have administrative privileges on other tier zero objects.

Kerberos Issues

-The Kerberos issues found in this domain are thankfully easy to resolve as well, despite the complexity of Kerberos itself. Marking tier zero users as “sensitive and cannot be delegated” and requiring them to have very long passwords will prevent the vulnerabilities found here from being exploitable by malicious actors.

CONCLUSION

This project explored four categories of attack paths that can exist within an Active Directory environment: cross-tier contamination, default permissions, excessive privileges, and Kerberos issues. Each of these categories represents a collection of specific attack paths identified by Bloodhound, which were then simulated in an offline test environment, exploited one by one, and then remediated through various means. The most important aspect of AD internal security is to carefully manage the tier zero objects, because these accounts and devices have the ability to manage identity and permissions through the whole environment, making them immensely valuable to a malicious actor.

REFERENCES

1. DagmarHeidecker. “Protecting Tier 0 the Modern Way.” Microsoft community Core Infrastructure and Security Blog. February 19, 2024. [Online]. Available: https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/protecting-tier-0-the-modern-way/ba-p/4052851

FUTURE WORK

Other projects in the future could explore different attack paths, depending on what vulnerabilities exist in domains other than the one analyzed here. It is possible that these other attack paths could be grouped into one of the four categories defined here, but it is also possible that they may need a new categorization altogether. After these specific attack paths are remediated, another analysis should be performed to see if any more vulnerabilities can be identified.