**Active Directory Attacks**

By Buwaneka Hettiarachchi

SID 104376165

Project 1 – RIS502

November 5, 2021

Table of Contents

[**Executive Summary** 2](#_Toc86971599)

[**Engagement Methodologies** 2](#_Toc86971600)

[**Attack Narrative** 2](#_Toc86971601)

[**Kerberoasting** 2](#_Toc86971602)

[**Silver Ticket Attack** 7](#_Toc86971603)

[**Golden Ticket Attack** 9](#_Toc86971604)

[**Technical Observations** 11](#_Toc86971605)

[**Kerberoasting** 11](#_Toc86971606)

[**Silver Ticket Attack** 11](#_Toc86971607)

[**Golden Ticket Attack** 12](#_Toc86971608)

[**References** 13](#_Toc86971609)

[Figure 1: Creating the normal user account 3](#_Toc86971612)

[Figure 2: Applying A service Principal Name for the User 3](#_Toc86971613)

[Figure 3: Kali Machine Uses Impact to discover the SPN 4](#_Toc86971614)

[Figure 4: Performing the Kerberoasting Attack using the wordlist 5](#_Toc86971615)

[Figure 5: Successfully Found the password Using the Hash cat 5](#_Toc86971616)

[Figure 6: Created a Ticket using mimikatz 6](#_Toc86971617)

[Figure 7: Successfully Extracted the Password using mimikatz 7](#_Toc86971618)

[Figure 8: Created and NLTM hash for the password 8](#_Toc86971619)

[Figure 9: Successfully Generated a Silver Ticket but failed to Attack 8](#_Toc86971620)

[Figure 10: Grabbing the User information of the KRBTGT user 9](#_Toc86971621)

[Figure 11: Successfully Generate the golden ticket 10](#_Toc86971622)

[Figure 12: Entered the Domain Controller using the Golden Ticket 10](#_Toc86971623)

# **Executive Summary**

The Goals and objective in this practical environment was to successfully create a lab environment that is capable of running Kerberos environment and then successfully generate three different attacks on the lab environment. Kerberos is a network authentication protocol that is used to provide strong authentication for clients and server applications through the use of secret-key cryptography. The attacks provided in this report are Kerberoasting, Silver Ticket Attack, and the Golden Ticket Attack and it will be further explained through the use practical walkthrough of each attack. The practical engagement started on October 29,2021 and testing went through for seven days until November 4, 2021. The Systems that were tested in the practical engagement were a Windows Server 2019 machine that hosted as an Active directory with an administrative account and a normal user account built into the server environment with addition of a Kali Linux machine used as a Remote machine for the purpose of pen testing. The results from the practical engagement came out as moderately successful where two of the attacks were perfectly executed while one attack had issues that were present within the environment this information will be further explained going through the report.

# **Engagement Methodologies**

Before doing the testing on the all the machines, it was my duty to fully understand that the Active directory has all the necessary plugins and do additional research on all the attacks so that all the necessary applications for each attack will be installed prior to the actual penetration testing on these types of attacks. The types of attacks that are interesting are the Silver Ticket attack and the Kerberoasting Attack, mainly due to the Silver Ticket Attack being one of the most difficult attacks to mitigate and Respond and for the Kerberoasting attack it is because we need to find many ways of extracting information using that attack.

# **Attack Narrative**

## **Kerberoasting**

The Attack was executed in a fully virtualized Environment, I worked on my Attacking phase by starting the Execute the first the Attack which was the Kerberoasting Attack. Before Starting to work on the Attack, I needed to create a normal user in the Active Directory and use it as the target machine for the attack. After creating the user with a custom password, I created a Service Principal Name (which is a unique service instance identifier used by Kerberos) on the created user.

A screenshot of a computer

Description automatically generated

Figure 1: Creating the normal user account

A screenshot of a computer

Description automatically generated

Figure 2: Applying A service Principal Name for the User

After creating the user in the Active Directory, I connected my Kali machine into the Network and started a connection to the Active Directory. Then, by using the impacket-GetUserSPNs command, I was able to grab information of the SPN I created and then I requested a Hash variable of the SPN and then put it into a hash file. After putting it into the Hash file, I proceeded to use the Hash cat plugin form Kali and through the use of a wordlist I was able to Extract the Password information of the created user.

A screenshot of a computer

Description automatically generated

Figure : Kali Machine Uses Impact to discover the SPN

As shown in the above Figure, we see that the Hash function uses the value krb5tgs 23. This means that the SPN hash function is given under Kerberos TGS repository and the type that they are using is the type 23. This information is useful because when Executing the attack, you will need information on how you will be able to extract the Kerberos Hash. This is shown in the figure below where it shows that hash cat uses the type 13100 which is used to extracting this type of Hash values.

A screenshot of a computer

Description automatically generated

Figure : Performing the Kerberoasting Attack using the wordlist

A screenshot of a computer

Description automatically generated with medium confidence

Figure : Successfully Found the password Using the Hash cat

The second method to the Kerberoasting Attack that I performed was through the use of mimikatz, which is plugin that I already installed in the Administrative account of the Active Directory. Mimikatz is an exploitation tool famous for using to dump password from the memory. This method of Kerberoasting Attack will export tickets when we add in the Service Principle Names into the PowerShell and start running the mimikatz service on the Active directory. After selecting the proper Ticket that correlates the user SPN, I would perform a python command where I installed a python file known as (tgsrepcrack.py) which is a python script that is used for extracting the Tickets that were exported by the Mimikatz. After running the python command, I extracted the password using the second method of Kerberoasting. After performing the Kerberoasting Attack I proceeded to work on the Silver Ticket Attack.

A screenshot of a computer

Description automatically generated

Figure : Created a Ticket using mimikatz

As shown in the Above figure it shows that mimikatz has exported more than one ticket, and if we closely look into it, we can come identify the ticket that we will be using through the use of Server Name, which is equal to the SPN of the User that you created.

A screenshot of a computer

Description automatically generated

Figure : Successfully Extracted the Password using mimikatz

## **Silver Ticket Attack**

To perform the Silver Ticket Attack we need to use mimikatz to generate the Silver ticket. To generate the Ticket, we need information such as the SID, Domain, target machine, service used by the machine, the NLTM hash of the password of the target machine, and a fake username that states the machine has been pawned. In this scenario, the target machine was the user that I created, and I used the same password that I extracted from the Kerberoasting Attack. After running the Kerberos command, I have successfully generated a Silver Ticket and to use the silver ticket I will be using on the target machine’s SQL server which needs to be installed prior to the attack and by running the command “sqlcmd -S (Target machine name)” you should get an SQL query terminal and by running the command “SELECT SERVER\_USERS” instead of the of the target machine name, you would get the fake username which means that the Silver ticket Attack was successful. But in this scenario, I wasn’t able to fully perform the Silver ticket properly. After proceeding with the Silver Ticket Attack, I will be working on the Golden Ticket Attack.

A screenshot of a computer

Description automatically generated with medium confidence

Figure : Created and NLTM hash for the password

A screenshot of a computer

Description automatically generated

Figure : Successfully Generated a Silver Ticket but failed to Attack

## **Golden Ticket Attack**

The Golden Ticket Attack will be focused more on getting access to the most powerful user account in the active directory which is known as the KRBTGT account. To do this attack, I logged in as the user I created and performed the attack from that user machine, we will use the mimikatz tool one more time for this attack and to generate a Golden Ticket, we need the NLTM hash of the KRBTGT account and the SID number of it as well. After grabbing that information, we can successfully generate a golden ticket. By running the “misc::cmd” in the mimikatz terminal, you will be redirected into the command prompt of the user and by running the command “pushd \\(computername)\c$”, you will be able to get access to the domain controller.

A screenshot of a computer

Description automatically generated

Figure : Grabbing the User information of the KRBTGT user

To discover the information of the KRBTGT account, we need information such as the Service ID and the NLTM hash values of the password. The above figure shows how the data was extracted. TO find the SID number we need to import the Active directory module into the PowerShell and then put in the command “get-aduser (username)” this will give a detailed explanation of the SID numbers of the KRBTGT account. To find the NLTM hash, you need to simply open mimikatz and use the command “lsadump::lsa /inject /name:krbtgt”, this command will provide you with the necessary details about the NLTM hash functions of the user. To perform the Golden Ticket Attack, we only need the SID number, the NLTM hash function, and Domain name of the server, if we have all the information necessary, we are ready to generate a Golden ticket.

A screenshot of a computer

Description automatically generated

Figure : Successfully Generate the golden ticket

A screenshot of a computer

Description automatically generated

Figure : Entered the Domain Controller using the Golden Ticket

# **Technical Observations**

## **Kerberoasting**

**Severity rating**

The Kerberoasting Attack is mediocre in terms of severity because it is easy to detect these attacks and respond to them, but to mitigate these attacks it is a bit difficult.

**Observations**

From the observations of the attack, both the methods require for the attacker to have a wordlist to identify the password of the account. This means that there is a certain level of brute forcing that require with finding the correct Password for the account and that is a bit time consuming.

**Impact**

An attacker can easily extract credentials hashes from and service accounts within the domain and does not need to use packets do it. This means that many service accounts are in then danger of being attacked due to their SPN.

**Recommendations**

Some ways to mitigate Kerberoasting attacks are by Enabling AES Kerberos Encryption, which has a stronger encryption method than the RC4 encryption. Having Group managed Service Accounts instead of the service accounts with static passwords will help to mitigate Kerberoasting.

## **Silver Ticket Attack**

**Severity rating**

While it is easier to Respond to these types of attacks, it is harder to Detect and Mitigate Silver Ticket Attacks.

**Observations**

To start off, this attack still needs the help of Kerberoasting, which enables it to find the password that it is looking for. For this attack to properly work, the user must run a service that the attack can occur on. In this report that attack focused on the SQL service. Unlike the golden ticket, the Silver ticket only

**Impact**

An attacker can easily gain control over a Domain Admin account in an Active Directory environment and then they can easily grant tickets to provide access to a single service on the Application.

**Recommendations**

Some mitigation points for Silver ticket attack is to ensure the principle of least privilege is in place for all the user accounts and provide awareness on these types of attacks to working employees.

## **Golden Ticket Attack**

**Severity rating**

It is very difficult to Detect and respond to this attack, but there is a mediocre level in mitigating the attack

**Observations**

For this attack to properly work, the attacker must need to identify the SID number and the hash of value of it.

**Impact**

The Golden Ticket Attack has a major impact because unlike the Silver Ticket where the attacker gains access to only a service in the application, this attack gives the attacker the complete access to the entire domain.

**Recommendations**

Create endpoints that limit attackers into opening modules such as mimikatz in the environment and Enforce the model of least privilege.

# **References**

https://attack.stealthbits.com/how-golden-ticket-attack-works

https://attack.stealthbits.com/silver-ticket-attack-forged-service-tickets

https://stealthbits.com/blog/impersonating-service-accounts-with-silver-tickets/

https://stealthbits.com/blog/complete-domain-compromise-with-golden-tickets/

https://attack.stealthbits.com/cracking-kerberos-tgs-tickets-using-kerberoasting

https://stealthbits.com/blog/extracting-service-account-passwords-with-kerberoasting/

https://www.varonis.com/blog/kerberos-how-to-stop-golden-tickets/