Windows Pass-the-ticket attack

The Kerberos Golden ticket

1 Introduction
Kerberos authentication protocol is nowadays the preferred authentication mechanism used by Windows in a domain-based environment. Although the pass-the-hash technique (PTH) is still prevalent in Advanced Persistent Threats (APT), the equivalent attack abusing the Kerberos protocol, known as pass-the-ticket (PtT), is more and more used.

A recent release of Mimikatz provides a proof of concept of an extension of the pass-the-ticket attack called the golden ticket. A golden-ticket enables the adversary to impersonate anybody in a Windows-domain based environment for an unlimited period of time.

This white-paper provides the required steps to prevent and block attacks based on the golden-ticket.

The tests mentioned in this document were done in a Windows 7 and Windows Server 2008R2 environment. New security controls have been put in place in Windows 8 and 2012R2 which mitigate the risks described in this paper. See [4] for further details. However, CERT-EU strongly recommends putting in place the controls described in this paper.

2 The golden ticket

2.1 What is a golden ticket
Mimikatz is a tool used by security researchers for pen-testing and studies purposes. It is publicly available and can potentially also be used with malicious intent.

The tool can dump Windows credentials, like NT hashes and Kerberos tickets, from memory and perform pass-the-hash and pass-the-ticket attacks. A recent release of mimikatz includes a new feature called golden ticket. This feature allows creating a special Kerberos TGT ticket which has the following properties:

- the golden ticket is a method to arbitrarily generate Kerberos TGT tickets for any user of the target domain. Therefore, it can be used to impersonate anybody, Domain Administrators accounts are the most interesting but potentially any legitimate user can be impersonated;
- golden tickets can be created off-line. Therefore, one does not need to be connected to the domain once you have collected all the data required to create the ticket (see next section);
- the golden ticket is valid for an arbitrary lifetime, mimikatz default is 10 years. This is the current setting implemented by mimikatz but it should be possible to create tickets of any lifetime at anytime (arbitrary start, renewal and end time is possible);
- Kerberos lifetime policy (default renewal lifetime 10h and total lifetime is 7 days) does not have any impact on the golden ticket. Indeed, KDC validates TGT tickets based on the lifetime settings embedded in the protected core of the ticket and not on the policy set on the Domain Controller.

---

1 Refer to [1] for more details about credential theft attacks, like pass-the-hash or pass-the-ticket. You can also find a short explanation in Annex A - Definitions and Annex B – Introduction to pass-the-ticket.
3 Refer to Annex B – Introduction to pass-the-ticket for an short explanation of this type of attack.
4 We extended the definition given by the author of Mimikatz as per the conclusions from the test performed in our lab. Specially, Mimikatz parameter ask for an admin user name to generate the golden ticket (/admin), however we have successfully generated and used tickets for any user.
Nevertheless, even if such control is in place, it cannot be used to block golden tickets. The attacker can generate any ticket with the appropriate lifetime in line with the local policy and so bypass the control:
- once created, the golden ticket can be replayed with pass-the-ticket attack technique. This will allow the adversary accessing other resources available to the impersonated user;
- as any pass-the-ticket, there is no need of privilege access to replay and use the golden ticket;
- resetting the password of the impersonated account does not make the golden ticket invalid;
- Windows event logs does not distinguish the use of legitimate TGT ticket versus a golden ticket, so there is no universal rule to detect the use of a golden ticket;

Example of a golden ticket with life time until 2024:

![Golden Ticket Image]

2.2 Requirements for golden ticket
This is the list of items required to create the golden ticket:

- the NTLM hash of the domain KRBTGT account:
  
  this hash is only hosted in the Active Directory of the Domain Controller. Therefore, the adversary must have compromised the Domain Controller first. This can be achieved with lateral movements like described in Annex B – Introduction to pass-the-ticket. Example of a KRBTGT hash:

  | KRBTGT:502:NO PASSWORD***********:a54932c2b0560e12386a0214767fbd5c::: |

- the targeted domain account name, usually a domain admin;
- the Domain name, this is trivial to obtain once the attacker has access to a host in the domain;
- the domain’s SID:
  
This can be obtained from a domain user SID or MS Sysinternals’ psGetsid.exe.

3 Countermeasures against the golden ticket

3.1 Prevention by protecting the DC and sensitive accounts
The main requirement to create a golden ticket is NT hash of the KRBTGT account which implies having access to the Domain Controller. This is often achieved by stealing sensitive domain accounts and doing lateral movement with pass-the-hash or pass-the-ticket attacks as explained in Annex B – Introduction to pass-the-ticket.

Microsoft has released a white paper that provides the controls to put in place to protect your domain against credential-theft-based attacks. The proposed countermeasures require a re-engineering of your Domain Controller and its management but we strongly recommend implementing them. Indeed, pass-the-[credential] attacks are always used in APTs and Domain Controller is one of their main targets.

3.2 Containment by resetting twice the KRBTGT account password

As mentioned earlier, resetting the password of the impersonated users does not block the usage of the related golden ticket. However, resetting twice the built-in Key Distribution Service account (KRBTGT) password will make invalid any golden tickets created with the previously stolen KRBTGT hash as well as all other Kerberos tickets.

3.2.1 Reasoning

The following simplified steps describe the Kerberos protocol when requesting access to a resource:

1. The requestor authenticates to the KDC. If the authentication is successful, the KDC creates the TGT ticket and encrypts the core of the TGT ticket with the NTLM hash of KRBTGT account before sending it back to the requestor.
   Note that this step is optional if a valid TGT ticket is already in memory (SSO feature) of the requestor host;
2. The TGT ticket does not provide direct access to a resource. The requestor send first the TGT ticket to the KDC to request a Service Ticket for the specific resource (ex, remote host);
3. The KDC decrypts the core of TGT ticket with its NTLM hash, If the KDC fails to decrypt with the NTLM hash, it will try with the former hashes stored in the Active Directory (i.e. the password history feature);
4. The KDC validates the content before creating and issuing the related Service Ticket (ST) to the requestor; If this latter step succeed, the requestor will send the ST to the resource to be accessed (ex, to the remote host of step 2);

Consequently, changing the KRBTGT account password\(^5\) will make the step-2 fail. In addition, as the KDC retries with former hashes, the golden ticket will be invalid only if the whole history of password is reset, 2 by default.

3.2.2 Impact

Changing the KRBTGT account hash may have an impact on the availability of legitimate session used by account in the target domain. The exact impact level will depend on the criticality of the related users, services and application. Here are some examples:

- End-users including smart-card users will be automatically requested to authenticate to receive a new valid ticket. This might create some load on the Domain controller;
- Services and applications that require manual startup with a password and use Kerberos may stop working properly until next manual restart.

Consequently, it is recommended to do a first assessment before resetting the KRBTGT account password.

3.2.3 How to reset KRBTGT account password

The following instructions depicts the way to reset the KRBTGT account password in a Domain Controller (Windows Server 2008):

1. open Active Directory Users and Computers on you Domain Controller;
2. Select Advanced Features in View menu;
3. Select Users in the target domain and find the KRBTGT user account;
4. Right-click the account, and then click “Reset password”;
5. Uncheck all options and enter the new password twice;
6. Redo step 4 and 5 to reset the password a second time;

---

\(^5\) NTLM hash is directly computed from the password.
3.3 Eradication by recovering your Domain Controller
As the domain controller is accessed to extract the required NT hash of the KRBTGT account, the usual procedure to recover from compromised Active Directory applies here.

CERT-EU recommends following your recovery procedure. We also recommend to read Microsoft guideline [3] Chapter 3 - Recovering from Active Directory Attacks.

3.4 Detection

3.4.1 Security events when using a valid golden tickets
As any pass-the-ticket attack, the attacker replays the golden ticket in a standard Kerberos protocol. Therefore, there is no clear indication of such attack in Windows logs. Nevertheless, general rules to detect pass-the-ticket attacks can be applied here. Another white-paper will be released soon on this subject.

3.4.2 Windows Security event after resetting KRBTGT password
The following event-id 4769 (A Kerberos service ticket was requested) is generated on the Domain Control when using a golden ticket after the double reset of the KRBTGT password. The status code 0x1f indicates a failed attempt with the following reason:

0x1f: Integrity check on decrypted field failed

Unfortunately, there is no additional information like the username linked to the TGT ticket or the resource that was requested. Consequently, the monitoring of this event is very limited and cannot be used efficiently to detect a potential use of a golden ticket.

Nevertheless, this type of error should be rare and might be worth to monitor and investigate.
Event id: 4769 - A Kerberos service ticket was requested.

Account Information:
- Account Name: 
- Account Domain: 
- Logon GUID: (00000000-0000-0000-0000-000000000000)

Service Information:
- Service Name: 
- Service ID: NULL SID

Network Information:
- Client Address: ::ffff:192.168.89.101
- Client Port: 49278

Additional Information:
- Ticket Options: 0x40810000
- Ticket Encryption Type: 0xffffffff
- Failure Code: 0x1f
- Transited Services:

### 4 Conclusion

The golden ticket is a real threat and is a dangerous asset in APTs:

- Attackers can use the technique to impersonate anybody in the domain and gain access to sensitive resources;
- They also gain immediate privilege access in the domain after a first eradicated wave of attack. Indeed, if during a first eradicated wave of attack, the adversary was able to get a copy of the Active Directory and this KRBTGT account password has not been properly reset, this same entity can immediately get privileged access in a second wave of attack. Only a simple but successful spear-phishing attempt against one internal workstation would be enough to gain again full control in a domain. There is no need of a privilege account on the local host to perform a pass-the-ticket attack.

We recommend the following guideline to protect against this type of attack:

- Prevention by protecting the DC and sensitive accounts (section 3.1);
- Containment by resetting twice the KRBTGT account password (section 3.2);
- Potentially detect the attack by monitoring event 4769 with error code 0x1f (section 3.4.2). However, this event may lead to false-positives;

### 5 Annex A - Definitions

**Pass-the-hash**: is a hacking technique that allows an attacker to authenticate to a remote server/service by using the previously stolen underlying NTLM and/or LanMan hash of a user’s password, instead of requiring the associated plaintext password as is normally the case.

**Pass-the-ticket**: similar to Pass-the-hash but with Kerberos tickets instead of NTLM/LanMan hashes;

**Credentials**: the identity and the related secret (authenticator) that can be used to proof someone identity. Consequently, a type of credential is not limited to plaintext passwords but it can be a Windows NTLM hash or a Kerberos Ticket depending on the Windows Authentication protocol that is used. In some circumstances, Windows caches the credentials to provide the single-sign-on feature. This paper will focus on Kerberos ticket called Ticket-Granting-Tickets (TGT). See [1] for more details about Windows Credential types (table 4) and caching.

**TGT and ST tickets**: Ticket-Granting-Tickets (TGT) and Service Tickets are part of the Kerberos protocol, refer to section 3.2.1. for a short description of these tickets. For more details about Kerberos and related tickets see [2].

**KDC**: Key distribution Center.

---

6 This is the source IP address from where the ticket was used. In some circumstance, we have seen events with the same error code but without any IP address.
Key Distribution Service account (krbtgt): this is a built-in account in the Domain Controller used by the KDC. This account has an NTLM hash which is used to create Kerberos tickets.

6 Annex B – Introduction to pass-the-ticket
The golden ticket exploits the pass-the-ticket technique. We provide below a short introduction to pass-the-ticket.
Pass-the-[Kerberos]-ticket is a similar attack than pass-the-hash attack. In both cases, the attack is a 2-steps-based scenario:

1. Capture the credential from memory of a compromised host, the Kerberos ticket (TGT or ST) in this case. This scenario requires
   - having control on a compromised host in the target network. This is usually obtained via spear phishing.
   - having high privileges or sedebug privileges on the compromised host. A local privilege escalation vulnerability can be used for this if the compromised user does not have such privileges yet.
   The privilege will allow the attack to access the memory (ie, LSAss process) and extract the credentials.
   The attacker can then take any credential that is stored in memory. The most interesting ones are privileged accounts of your domain like help-desk or domain admin account.

2. Replay the ticket to access resources:
   Once the credential is stolen, the attacker can use it to access another resource like another host or server (ex, Exchange email accounts). This is called lateral movement.
   The advantage of this attack is that the attacker can capture a credential and use it later on with specialized tools like mimikatz.

It is important to note that those credentials, including domain admins one, are cached in memory of the workstation where they connected to or run commands, for instance when doing RDP or runas commands. Therefore if these privileged accounts are connected to an infected machine, their credentials are exposed. Usually, APTs will target other workstation where it can obtain higher and higher privilege accounts until they get the credential of a domain admin account. The final step of the attack will be to access the Domain Controller and get a copy of the entire Active Directory.
The following picture presents the typical scenario of an APT with lateral movement:
You can find more details about pass the hash/ticket and credential theft from memory in [1]. This document published by Microsoft provides as well counter-measures to protect your environment against such attack scenarios.

7 Annex C - References

Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques

Kerberos Authentication Technical Reference

Chapter 3 - Recovering from Active Directory Attacks

Credential Protection and Management