# Exercise -4: check tickets

1. The command “privilige::debug“ is used to allow the users to debug other processes on the system .

Text

Description automatically generated

1. In Mimikatz, the sekurlsa::logonpasswords command is used to extract login passwords from the memory of a Windows computer. When this command is run, Mimikatz will search the memory of the system for any stored login passwords and display them on the screen.\

The sekurlsa::logonpasswords command can be used to extract the passwords of users who are currently logged in to the system, as well as the passwords of users who have logged in to the system in the past. This can include the passwords of both local users and domain users.

Text

Description automatically generated

1. In Mimikatz, the kerberos::list command is used to display information about Kerberos tickets on a Windows system. When this command is run, Mimikatz will search the memory of the system for any stored Kerberos tickets and display information about them, including the service principal name (SPN), the client name, and the encryption type.

The sekurlsa::tickets command can be useful for extracting and examining Kerberos tickets on a system as part of a security assessment or for troubleshooting authentication issues.

Text

Description automatically generated

1. the sekurlsa::minidump command is used to extract login passwords and other sensitive information from a memory dump file.

A memory dump file is a file that contains a snapshot of the memory of a computer at a specific point in time. It can be used to troubleshoot problems with a computer or to examine the state of the system for security purposes.

To use the sekurlsa::minidump command, you must first create a memory dump file by using a tool such as the Windows Debugging Tools or by using the built-in Windows utility "Task Manager."

Once you have a memory dump file, you can use the sekurlsa::minidump command in Mimikatz to extract login passwords and other sensitive information from the file.



5. The kerberos::purge command can be useful for removing Kerberos tickets from the memory of a system as part of a security assessment or for troubleshooting authentication issues.



the event::clear command is used to clear the event log of a Windows system. The event log is a record of system and security events that have occurred on a computer. It can be used to troubleshoot problems with the system, to track security events, or to monitor the performance of the system.

.Text

Description automatically generated

7. This command takes several arguments, including the name of the domain, the name of the forged user, and the expiration date of the ticket. The attacker can then use the kerberos::ptt command to inject the ticket into the memory of the system.

a "golden ticket" is a type of forged Kerberos ticket that can be used to gain unauthorized access to resources on a Windows domain. A golden ticket is created by an attacker and contains forged information about a user, including their user principal name (UPN), security identifier (SID), and other attributes.

To submit a golden ticket, an attacker can use Mimikatz to inject the forged ticket into the memory of a Windows system. The attacker can then use the ticket to authenticate to services on the domain and access resources as if they were the forged user.

Text

Description automatically generated