Manipulating User Passwords with Mimikatz

blog.netwrix.com/2022/09/28/manipulating-user-passwords-with-mimikatz

Jeff Warren

Using the ChangeNTLM and SetNTLM commands in Mimikatz, attackers can manipulate user passwords and escalate their privileges in Active Directory. Let's take a look at these commands and what they do.

Handpicked related content:

[Free Guide] Active Directory Security Best Practices

ChangeNTLM

The ChangeNTLM command performs a password change. To use this command, you need to know the either the account's current password or its NTLM password hash, which can be much easier to steal than cleartext passwords. By default, the ability to change a user's password is granted to Everyone, so this command can be executed by any user without special privileges.

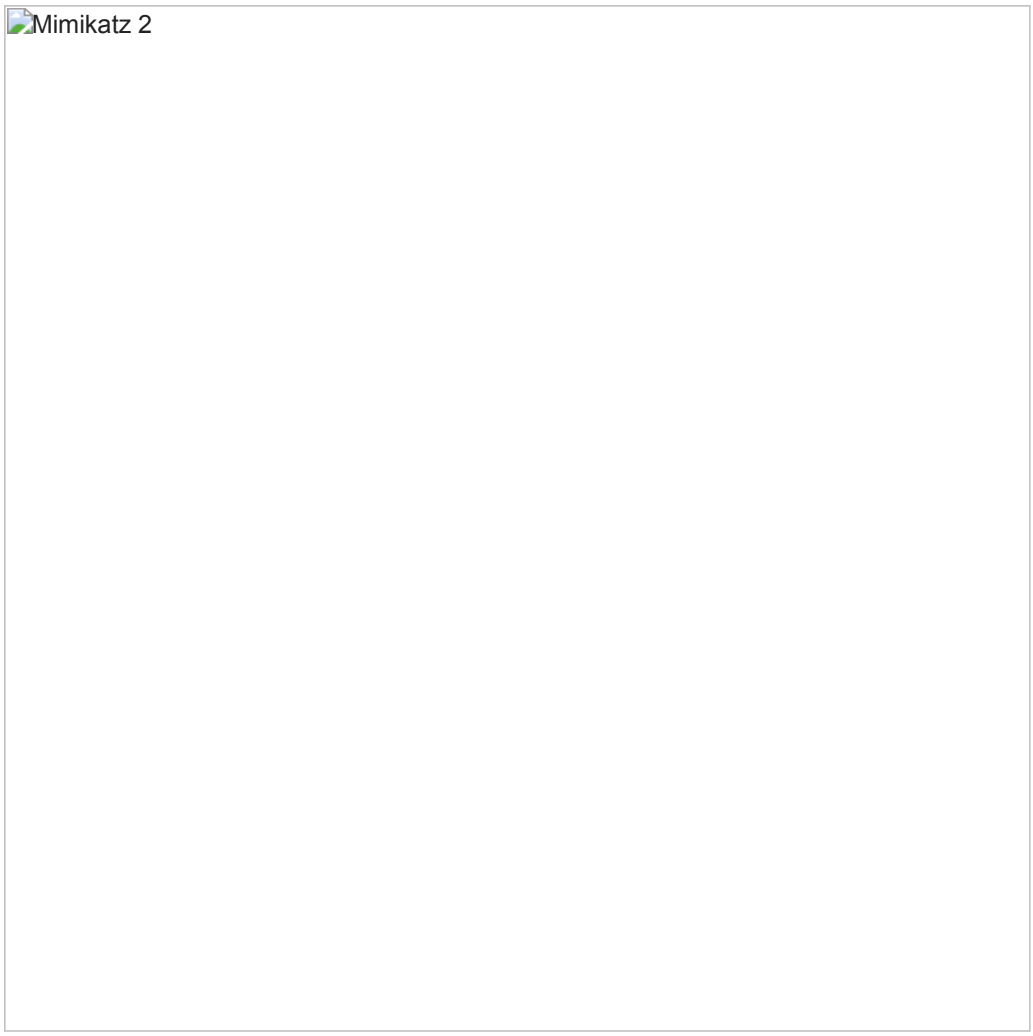
Here is an example of using the command to change a user's password knowing only the current password hash:

This will produce Event ID 4723 in the domain controller event log.

SetNTLM

This command performs a password reset. Executing it does not require you to know the user's current password, but it does require you to have the Reset Password right on the account, which is not granted to Everyone by default.

Here is an example of using the command to reset a user's password:



This will produce Event ID 4724 in the domain controller event log.

Attack Scenario: ChangeNTLM

Compromising a user's password hash enables an adversary to perform pass-the-hash attacks. However, those attacks are typically limited to command-line access to systems and applications. To log into Outlook Web Access (OWA), SharePoint or a remote desktop session, the adversary may need the user's cleartext password. They can perform the attack and cover their tracks in four quick steps:

1. Compromise an account's NTLM hash.
2. Change the password using the hash.
3. Use the new cleartext password to access the desired applications or services.
4. Set the password back to its previous value using the stolen hash.

This attack is very useful for further exploiting compromised accounts.

Attack Scenario: SetNTLM

In this scenario, an attacker has compromised an account with limited domain access and . Exploiting that attack path involves resetting user passwords to take over their accounts, but the attacker does not want to alert users to the fact that their account has been compromised by changing their password. How can the attacker reset the

users' passwords and then put them back to their old values once the target is compromised? Enter SetNTLM.

The attacker can follow this basic path:

1. Use Bloodhound to identify an attack path that leverages Active Directory permissions and password resets.
2. Exploit the attack path, resetting passwords as required.
3. Once privileged access is achieved, use Mimikatz to extract NTLM password history for all compromised accounts.
4. Use SetNTLM to apply the previous NTLM hashes to the accounts, setting the passwords back the way they were.

Note**:** The same can be done using the DSInternals Set-SamAccountPasswordHash command.

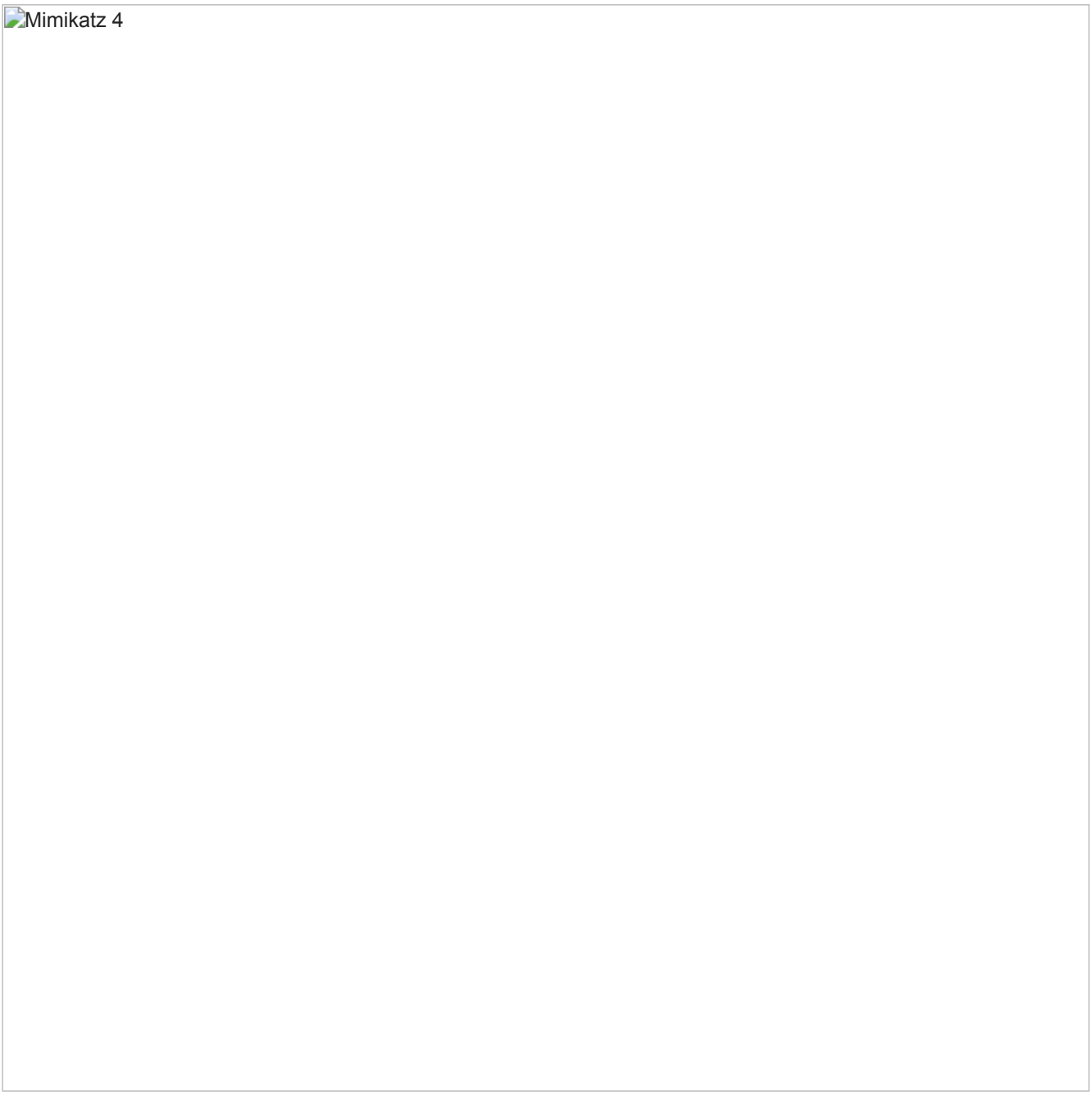
Example

Suppose we have the following attack path that will take us from our current user to Domain Admin in three password resets:

Now that we know which accounts need to be compromised, we want to execute the attack as quickly as possible to not alarm any users. We can script out the password reset attack path using some basic PowerShell. The following script will take a password and follow the attack chain, impersonating each compromised user along the way until reaching the goal of Domain Admin:

Next, we will launch a new PowerShell session as the Domain Admin and perform a DCSync operation to get the NTLM password history for all of the accounts:

From there, we will set the passwords back to their former values using the SetNTLM command:

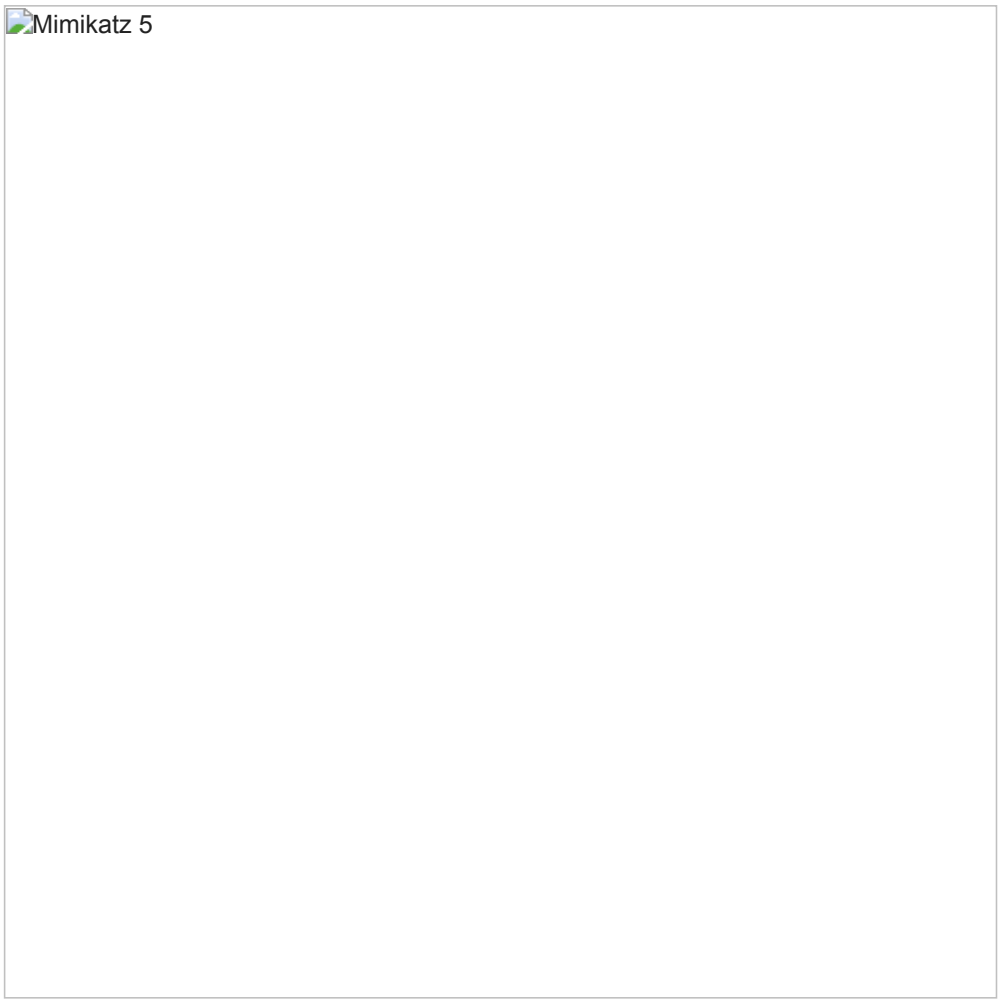


And there you have it. We now have become a Domain Admin and covered our tracks as best as we can to avoid users realizing their accounts have been compromised along the way.

Detecting and Preventing SetNTLM and ChangeNTLM Attacks

Detecting the Attacks

If an attacker uses the ChangeNTLM attack, this will generate a 4723 event, but the Subject and Target Account will be different, as shown below. This will stand out from normal password changes that users perform on their own, where the two values will be identical. If administrators are going to reset passwords, they will perform a reset and generate a 4724 event.



Preventing the Attacks

To mitigate the risk of SetNTLM attacks being executed, control password reset rights in the directory. To mitigate the risk of ChangeNTLM attacks, control how and where user hashes get stored.

How Netwrix Can Help

The Netwrix Active Directory Security Solution helps you secure your Active Directory from end to end — from highlighting security gaps in your current AD settings to detecting sophisticated attacks in real time and responding to threats instantly. It helps you to ensure all identities, the sensitive data they provide access to and the underlying AD infrastructure are clean, understood, properly configured, closely monitored and tightly controlled — making your life easier and the organization more secure.

Jeff Warren