Stealing Credentials with a Security Support Provider (SSP)

blog.netwrix.com/2023/02/24/security-support-provider-attacks

Jeff Warren

Mimikatz provides attackers with several different ways to steal credentials from memory or extract them from Active Directory. One of the most interesting options is the MemSSP command. An adversary can use this command to register a malicious Security Support Provider (SSP) on a Windows member server or domain controller (DC) — and that SSP will log all passwords in clear text for any users who log on locally to that system.

Handpicked related content:

Active Directory Security Best Practices

In this post, we will explore this attack and how attackers can use it to elevate their privileges.

SSP Attack Scenarios

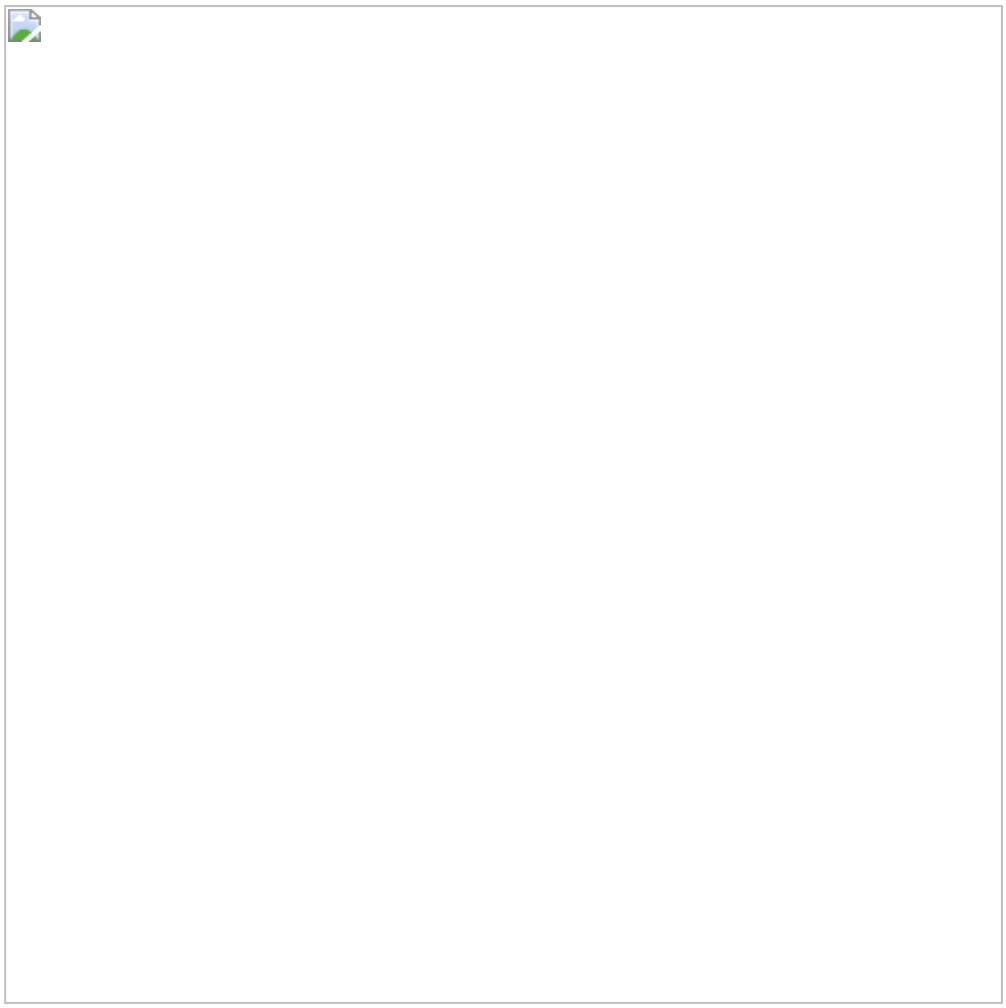
A Security Support Provider is a dynamic-link library (DLL) involved in security-related operations, including authentication. Microsoft provides a number of SSPs, including packages for Kerberos and NTLM. Let's look at some of the reasons an attacker might want to register a malicious SSP on a computer:

- An attacker has compromised a member server as a local Administrator but has limited rights to move laterally throughout the domain.
- An attacker has compromised a DC as a Domain Admin or Administrator but wants to elevate their privileges to Enterprise Admin to move laterally across domains.
- An attacker has compromised a DC as a Domain Admin using a Pass-the-Hash attack but wants to leverage the clear text password of the admin to log into other applications, such as Outlook Web Access or a remote desktop connection.

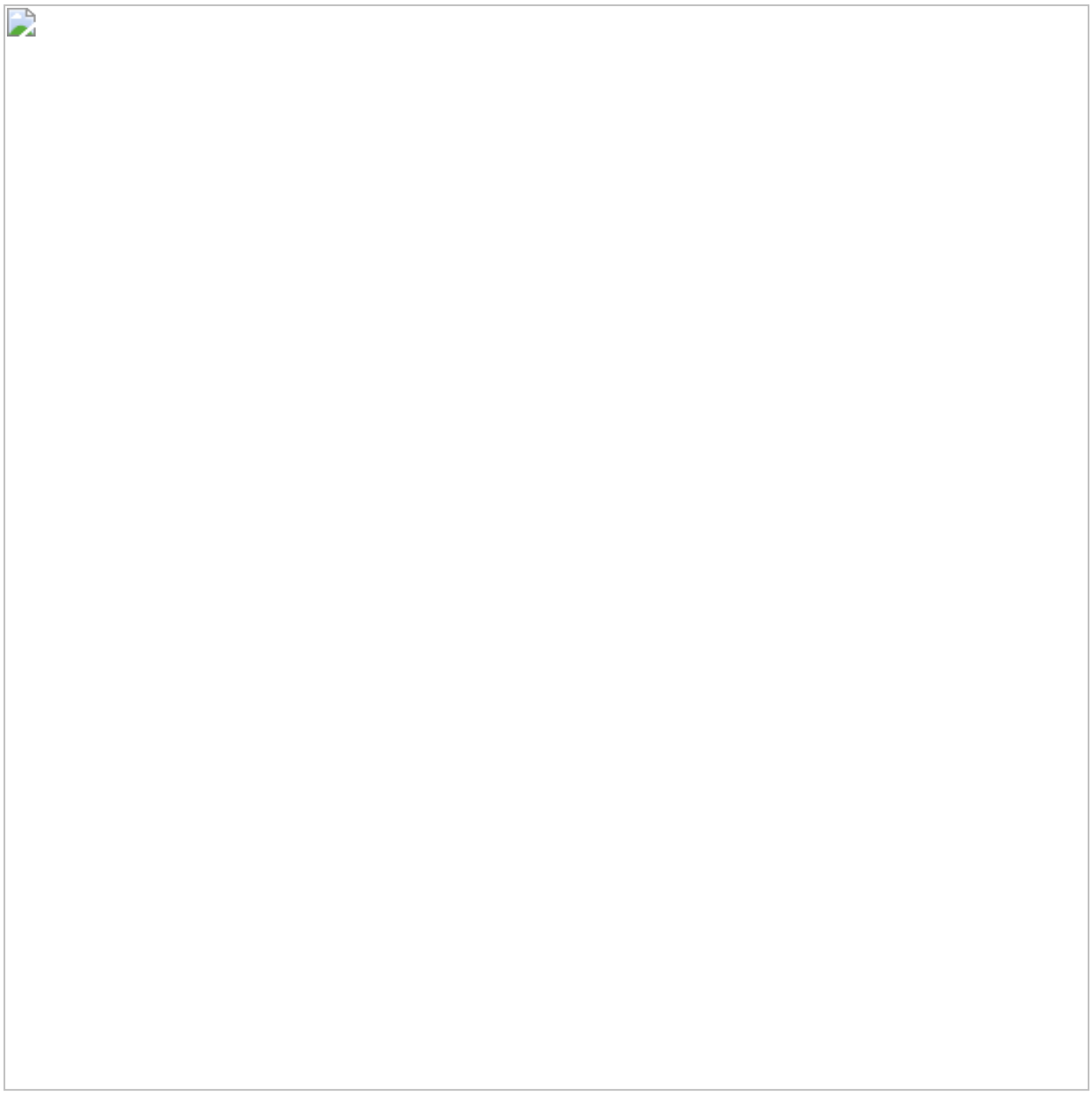
In any of these scenarios, an SSP attack can be very effective.

Performing an SSP Attack

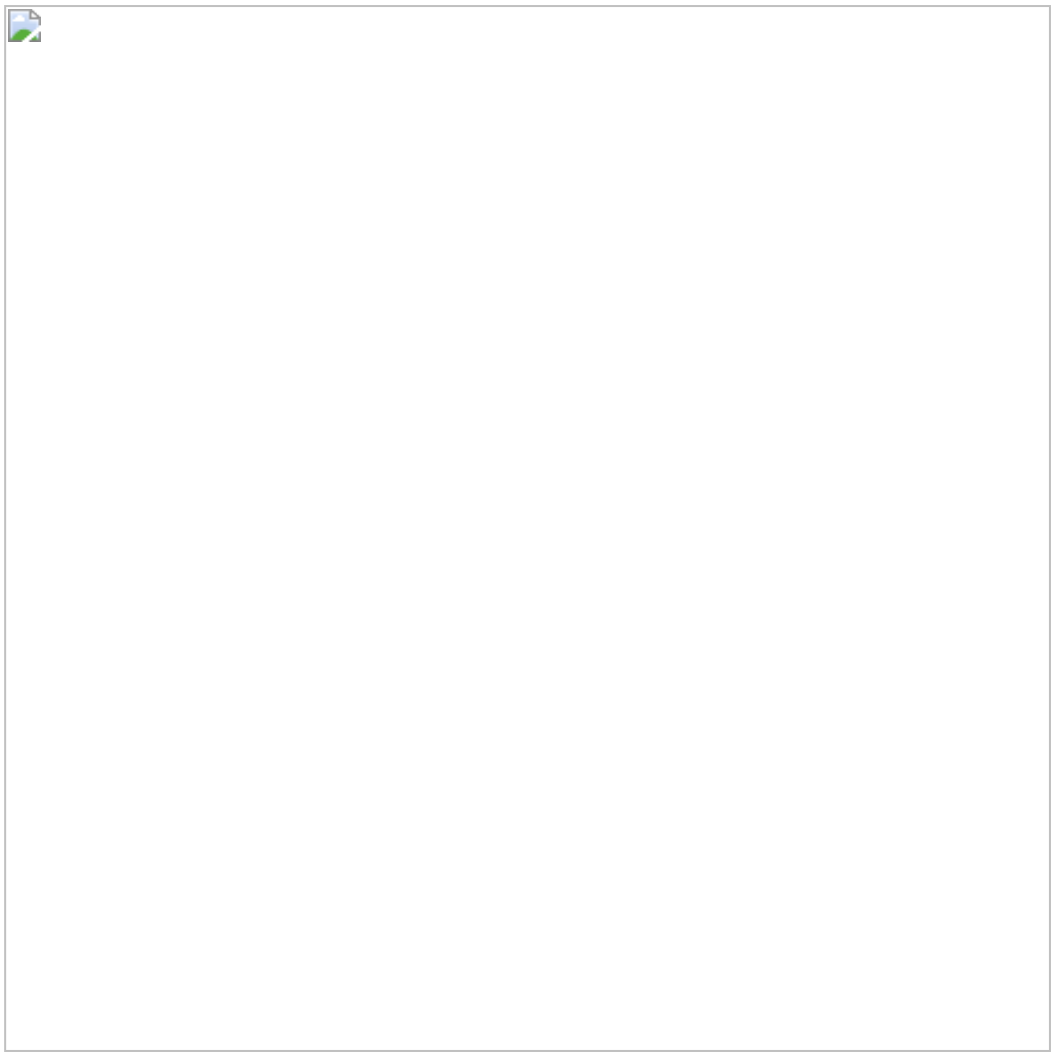
Performing an SSP attack is very simple. For this post, let's focus on the attacks that target a domain controller. Let's assume we have compromised a Domain Admin account and want to inject a malicious SSP into memory. All we need to do is issue the misc::memssp command in Mimikatz:



Now the SSP is injected into memory. However, if the DC is rebooted, the SSP will be lost and must be injected again. This can be solved by registering a DLL as an SSP that is provided with Mimikatz.



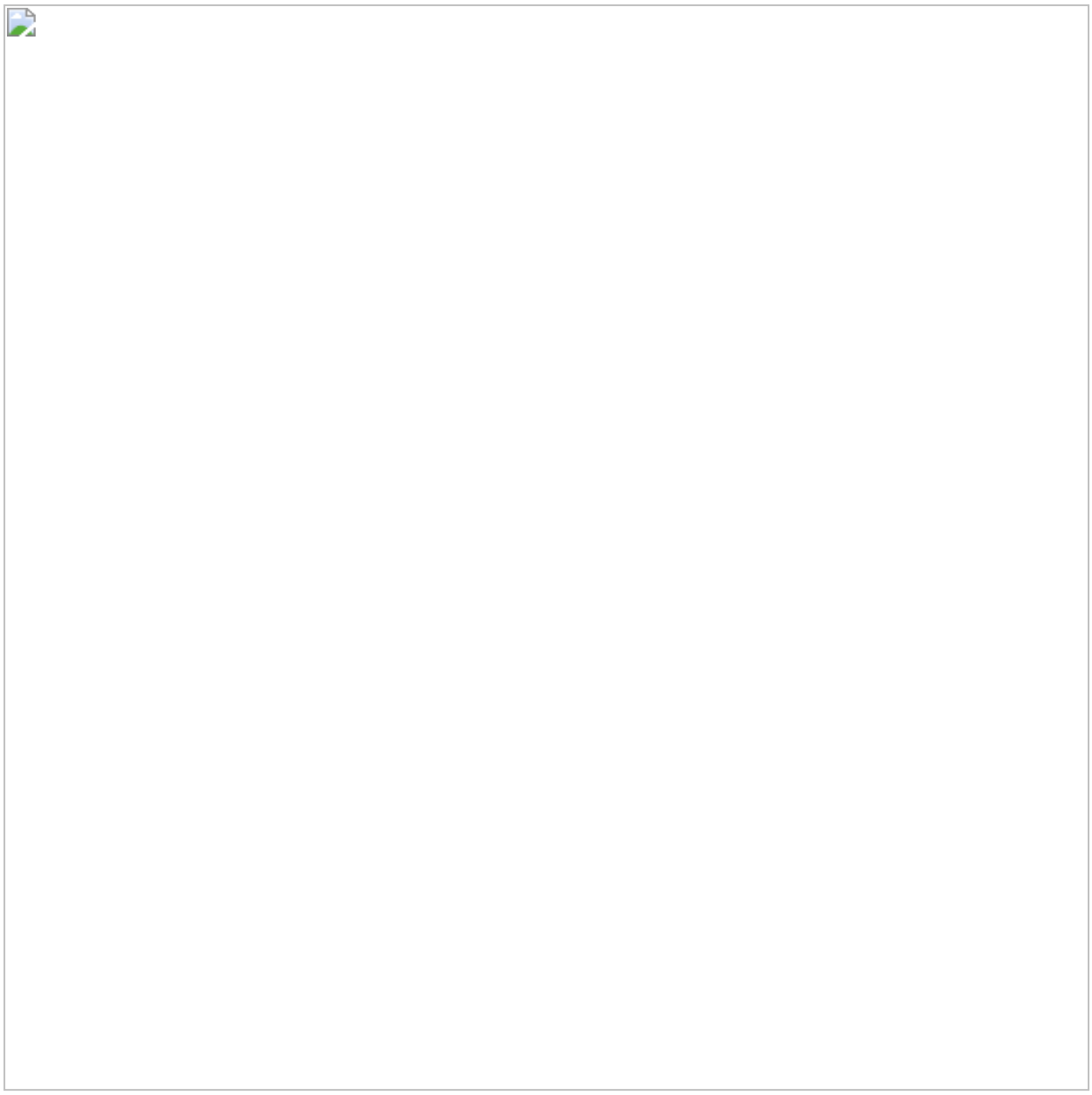
Once the SSP is registered, all users who log on to the DC, as well as all local services, will log their passwords to the c:WindowsSystem32mimilsa.log file. That file will contain the clear text passwords for all users who have logged on and service accounts running on the system:



Protecting Against SSP Attacks

Detection

SSP attacks can be difficult to detect. To see whether any of your DCs have already been compromised, you can run the following PowerShell command to check each DC in the domain for the existence of the mimilsa.log file. Hopefully, the results come back empty.



Prevention

Since SSP attacks on DCs require an attacker to have compromised the DC as a Domain Admin or Administrator, the best prevention is to keep those accounts from being compromised by strictly limiting membership in those groups, enforcing strong account governance and monitoring the activity of privileged accounts.

How Netwrix Can Help

Identify security issues in your environment and fix the gaps before bad actors exploit them using tools like Mimikatz with the Netwrix Active Directory security solution. It will enable you to:

- Uncover security risks in Active Directory and prioritize your mitigation efforts.
- Harden security configurations across your IT infrastructure.
- Promptly detect and contain even advanced threats, such as DCSync and Golden Ticket attacks.

- Respond to known threats instantly with automated response options.
- Minimize business disruptions with fast Active Directory recovery.

Jeff Warren