

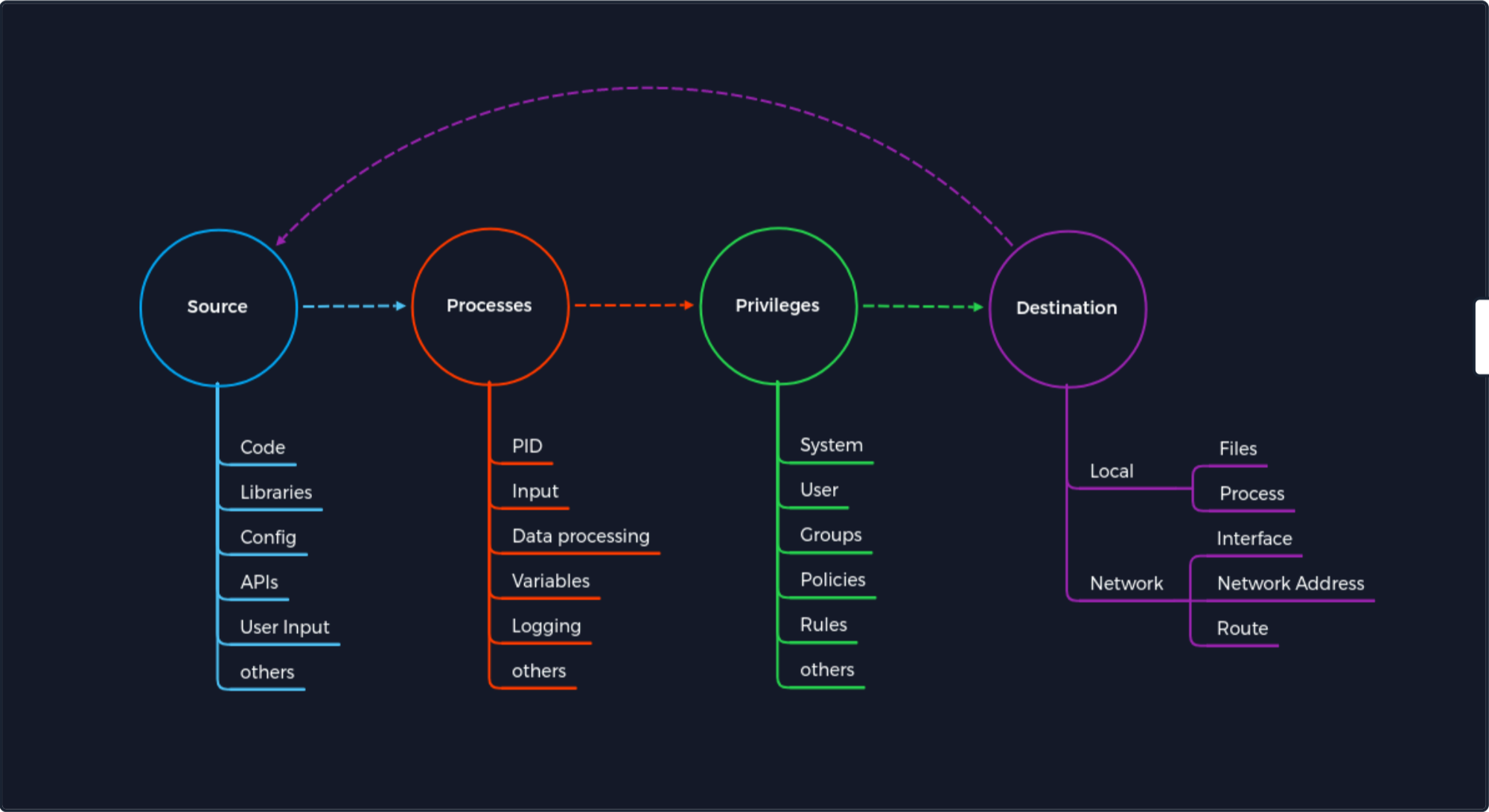
Latest SQL Vulnerabilities

This time let's discuss a vulnerability that does not have a CVE and does not require a direct exploit. The previous section shows that we can get the NTLMv2 hashes by interacting with the MSSQL server. However, we should mention again that this attack is possible through a direct connection to the MSSQL server and vulnerable web applications. However, we will only focus on the simpler variant for the time being, namely the direct interaction.

The Concept of the Attack

We will focus on the undocumented MSSQL server function called xp_dirtree for this vulnerability. This function is used to view the contents of a specific folder (local or remote). Furthermore, this function provides some additional parameters that can be specified. These include the depth, how far the function should go in the folder, and the actual target folder.

The Concept of Attacks



The interesting thing is that the MSSQL function xp_dirtree is not directly a vulnerability but takes advantage of the authentication mechanism of SMB. When we try to access a shared folder on the network with a Windows host, this Windows host automatically sends an NTLMv2 hash for authentication.

This hash can be used in various ways against the MSSQL server and other hosts in the co attack where we "replay" the hash to log into other systems where the account has local ac system. Successful cracking would allow us to see and use the password in cleartext. A su rights on another host in the network, but not necessarily the host where the hash originat allowed an SMB Relay back to the originating host. We could, however, possibly gain local that could be re-used to gain local admin access to the original system where the NTLMv2

4

Weekly Goal Complete! BETA

Your streak is now saved till next week.

30 / 30 Streak pts earned

Initiation of the Attack

		Concept of Attacks - Category
Step	XP_DIRTREE	
1.	The source here is the user input, which specifies the function and the folder shared in the network.	Source
2.	The process should ensure that all contents of the specified folder are displayed to the user.	Process
3.	The execution of system commands on the MSSQL server requires elevated privileges with which the service executes the commands.	Privileges
4.	The SMB service is used as the destination to which the specified information is forwarded.	Destination

This is when the cycle starts all over again, but this time to obtain the NTLMv2 hash of the MSSQL service user.

Steal The Hash

		Concept of Attacks - Category
Step	Stealing the Hash	
5.	Here, the SMB service receives the information about the specified order through the previous process of the MSSQL service.	Source
6.	The data is then processed, and the specified folder is queried for the contents.	Process
7.	The associated authentication hash is used accordingly since the MSSQL running user queries the service.	Privileges
8.	In this case, the destination for the authentication and query is the host we control and the shared folder on the network.	Destination

Finally, the hash is intercepted by tools like [Responder](#), [WireShark](#), or [TCPDump](#) and displayed to us, which we can try to use for our purposes. Apart from that, there are many different ways to execute commands in MSSQL. For example, another interesting method would be to execute Python code in a SQL query. We can find more about this in the [documentation](#) from Microsoft. However, this and other possibilities of what we can do with MSSQL will be discussed in another module.

← Previous

Next →

+10 Streak pts

✔ Mark Complete & Next

- Cheat Sheet
- Resources

Table of Contents

Introduction

Interacting with Common Services

✔

Protocol Specific Attacks

The Concept of Attacks

✔

Service Misconfigurations

Finding Sensitive Information

FTP

📦 Attacking FTP

Latest FTP Vulnerabilities

SMB

4

Weekly Goal Complete! BETA

Your streak is now saved till next week.

30 / 30 Streak pts earned

1

[illegible]

 Interact

✗ Terminate

 Reset

Life Left: 13m

+

4

Weekly Goal Complete! BETA

Your streak is now saved till next week.

30 / 30 Streak pts earned