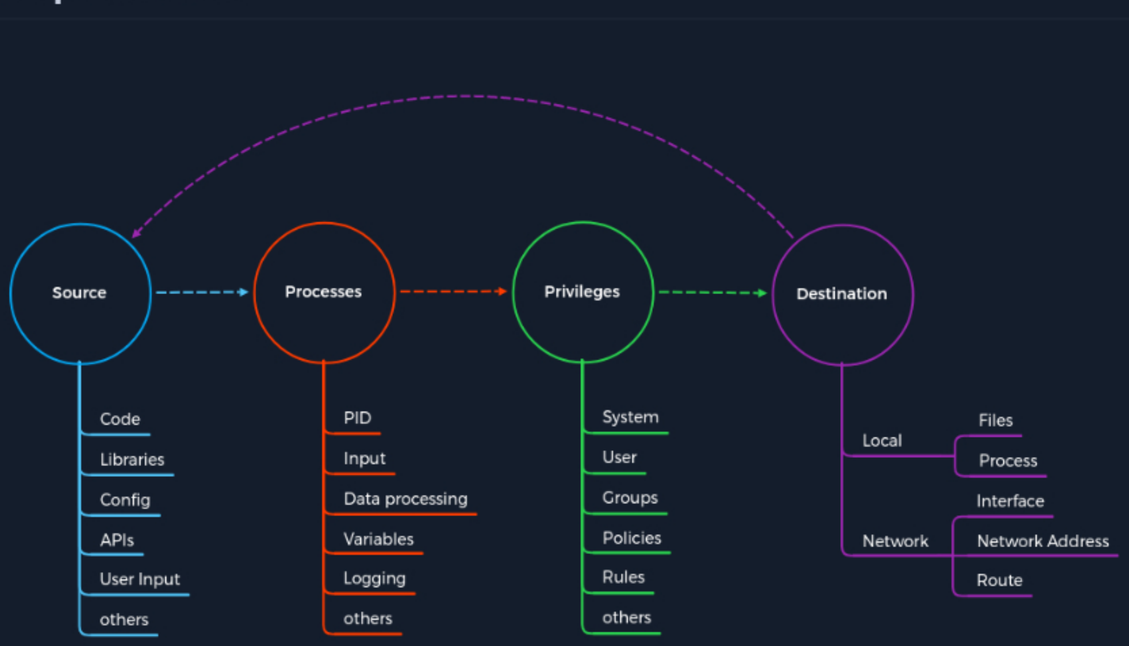
Latest RDP Vulnerabilities

In 2019, a critical vulnerability was published in the RDP (`TCP/3389`) service that also led to remote code execution (`RCE`) with the identifier CVE-2019-0708. This vulnerability is known as `BlueKeep`. It does not require prior access to the system to exploit the service for our purposes. However, the exploitation of this vulnerability led and still leads to many malware or ransomware attacks. Large organizations such as hospitals, whose software is only designed for specific versions and libraries, are particularly vulnerable to such attacks, as infrastructure maintenance is costly. Here, too, we will not go into minute detail about this vulnerability but rather keep the focus on the concept.

The Concept of the Attack

The vulnerability is also based, as with SMB, on manipulated requests sent to the targeted service. However, the dangerous thing here is that the vulnerability does not require user authentication to be triggered. Instead, the vulnerability occurs after initializing the connection when basic settings are exchanged between client and server. This is known as a Use-After-Free (`UAF`) technique that uses freed memory to execute arbitrary code.

The Concept of Attacks



This attack involves many different steps in the kernel of the operating system, which are not of great importance here for the time being to understand the concept behind it. After the function has been exploited and the memory has been freed, data is written to the kernel, which allows us to overwrite the kernel memory. This memory is used to write our instructions into the freed memory and let the CPU execute them. If we want to look at the technical analysis of the BlueKeep vulnerability, this article provides a nice overview.

Initiation of the Attack

Step	BlueKeep	Concept of Attacks - Category
1.	Here, the source is the initialization request of the settings exchange between server and client that the attacker has manipulated.	`Source`
2.	The request leads to a function used to create a virtual channel containing the vulnerability.	`Process`
3.	Since this service is suitable for administering of the system, it is automatically run with the LocalSystem Account privileges of the system.	`Privileges`
4.	The manipulation of the function redirects us to a kernel process.	`Destination`

This is when the cycle starts all over again, but this time to gain remote access to the target system.

Trigger Remote Code Execution

Step	BlueKeep	Concept of Attacks - Category
5.	The source this time is the payload created by the attacker that is inserted into the process to free the memory in the kernel and place our instructions.	`Source`
6.	The process in the kernel is triggered to free the kernel memory and let the CPU point to our code.	`Process`
7.	Since the kernel also runs with the highest possible privileges, the instructions we put into the freed kernel memory here are also executed with LocalSystem Account privileges.	`Privileges`
8.	With the execution of our instructions from the kernel, a reverse shell is sent over the network to our host.	`Destination`

Not all newer Windows variants are vulnerable to Bluekeep, according to Microsoft. Security updates for current Windows versions are available, and Microsoft has also provided updates for many older Windows versions that are no longer supported. Nevertheless, `950,000` Windows systems were identified as vulnerable to `Bluekeep` attacks in an initial scan in May 2019, and even today, about `a quarter` of those hosts are still vulnerable.

ⓘ Note: This is a flaw that we will likely run into during our penetration tests, but it can cause system instability, including a "blue screen of death (BSoD)," and we should be careful before using the associated exploit. If in doubt, it's best to first speak with our client so they understand the risks and then decide if they would like us to run the exploit or not.

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left