Make Null Session Great Again

sud0ru.ghost.io/make-null-session-great-again

Sud0Ru November 17, 2024

Nov 17, 2024 2 min read

It has been 24 years since the discovery of null sessions. Today, most system administrators actively prevent and detect their use by enforcing strict security policies. But after all these years, can we revive the concept of null sessions—or "no authentication"—in a way that bypasses these modern restrictions and policies?

In this blog post, you'll find a quick guide to my latest research, along with all the resources you need to understand the topic better.

As a result of this research, you'll discover a new method for enumerating domain information without authentication, specifically domain users. We'll also explore why this activity cannot be fully prevented, how it can be detected, and the reasons behind this Windows behavior. To explain this, I'll apply two analysis strategies and use reverse engineering on the Netlogon DLL.

The story began with research I published on the Kaspersky Securelist website, which you can check out here.

In the first part of the research, I shared the background and how it all began with the observation of interesting behavior in the IOXIDResolver interface. I introduced a new alternative path for null sessions, which I named the "no-auth path," allowing the use of authentication level one (no authentication) when binding the interface through the TCP transport layer.
I also explained the methodology, leveraging a combination of Impacket scripts to identify interfaces impacted by the no-auth path. As a result, I demonstrated how to enumerate domain information and domain users without authentication using the MS-NRPC protocol interface

Alongside publishing this research, I also presented a talk at the PHDays conference, which you can watch here. In this 35-minute talk, I presented the same research and further explored why this behavior cannot be prevented, while also outlining methods for its detection.
Additionally, I introduced a Python tool designed to enumerate domain information, including sites, forests, flags, trusted domains, domain users, and domain computers. You can check out the tool here: NauthNRPC.
I also published a Metasploit module for enumerating domain users, which you can find here: NRPC Enum Users. The second part of the research aimed to understand this behavior and how domain users can be enumerated without authentication.

I began by explaining the internals of RPC server security and the methods available to secure an RPC server. Using this knowledge, I developed two analysis approaches:

1. **Surface Analysis** – This involved applying theoretical knowledge to uncover initial insights.
2. **In-Depth Analysis** – Using reverse engineering with IDA on the Netlogon DLL, I sought deeper answers.

As a result, I discovered that the interface includes a security descriptor that permits anonymous users. Additionally, the server registers a security callback containing an access matrix, allowing remote access to specific functions within the interface. Among these functions are those used to retrieve information about the domain controller, which is how the enumeration was achieved. The white paper for the second part of the research you can see it here.

I presented a talk about The second part at the POC2024 conference.
You can check out the slides here. Hopefully, the recording will be available soon. This short blog post serves as a guide to bring everything together and help you get the most out of this research. I'll keep updating this guide as new information becomes available.

Thanks for reading, and I look forward to sharing more interesting topics with you soon!