Learn Null Session attacks

Null sessions, called IPC $ on a Windows platform server, are an anonymous connection to a shared network that allows users in the network to access freely.

***Network Administration* - Null Session, called IPC $ on a Windows platform server, is an anonymous connection to a shared network that allows users in the network to access freely.**

The null session attack has been around since Windows 2000 was widely used, however, this form of attack is not taken care of by system administrators when applying network security measures. This can lead to inconceivable outcomes because hackers can use this form of attack to get all the useful information needed to gain remote access to the system. Although not new, attack on null sessions is still as common and dangerous as in previous years. In some respects, although the security of modern systems is not too weak, when doing penetration tests on Windows computers, the results show that null sessions are still one of the form to note. In this article we will learn how the null session attacks work and how to prevent them from happening on the system.

Null Session operation method

A remote access session is established when a user logs on remotely to a computer using a username and password that has access to system resources. This login process is done via SMB (Server Message Block) and Windows Server services. These connections are completely legal when the correct login information is used.

A null session occurs when a user makes a connection to a Windows system without using a username or password. This form of connection cannot be performed on any regular Windows sharing form, but can be performed on IPC (Interprocess Communication) administrative sharing. IPC sharing is used by Windows processes (with the user name SYSTEM) to communicate with other processes over this network. IPC sharing is only used by the SMB protocol.

Sharing does not require login information. IPC is often used for programs that communicate with another program, but there is no guarantee that users cannot connect to a computer using this IPC connection. IPC connectivity not only allows unlimited access to computers, but also grants access to all computers on the network, and this is what hackers need to infiltrate the system.

Attack method using null sessions

Now that we know how to run null sessions, however, is it easy for hackers to use this attack? ' The answer is 'quite easy'. The Null Session connection can be set directly from a Windows command without using additional tools, which is the *NET* command. *NET* command can perform many administrative functions, when using this command we can create a connection to a standard share on the destination server, but this connection will fail due to login information. incorrect.

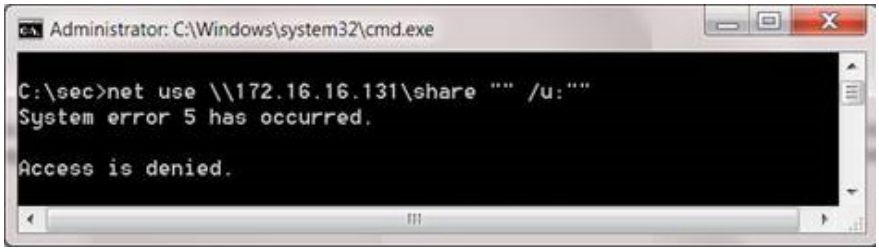

Figure 1: Connecting failures to a shared network using the NET command.

When using the *NET* command, we can change the shared name connected to the IPC $ admin sharing. Then the results will be better.

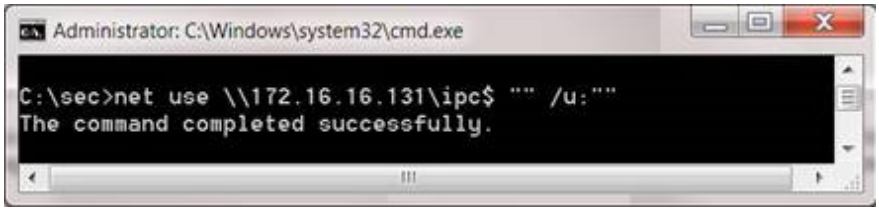

Figure 2: Connecting null sessions successfully with the NET command.

At this point, we have set up a null session connection to the victim computer. However, we still do not have administrative access on this computer, so we cannot start searching for hard drives or getting passwords. Remember, IPC sharing is used to communicate between processes, so our access will be limited to the access of the SYSTEM user name. We can use the NET command to get more information from the target computer, but there are many automation tools that will perform these troublesome tasks.

In this example, we will use the tool to retrieve information from null sessions named Enum. Enum is a free command line platform utility that can be used to get user names, group names, system information, etc. One of the most important information for hackers is the list of users on the system. . With this list, we can conduct password predictions and even apply password-breaking measures. To get a list of users with Enum, run the following command:

Figure 3: Use the Enum tool to get a list of users on the system.

With the list of users in hand, we can retrieve the system password policy to easily break the password.

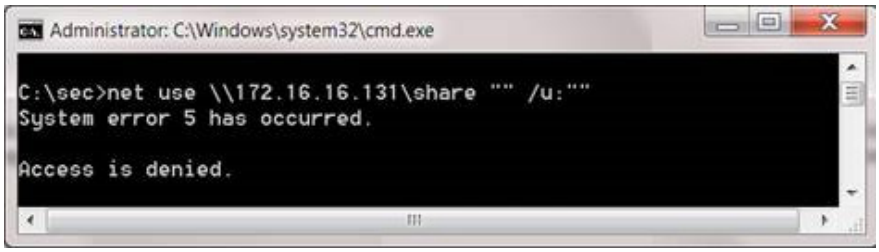

Figure 4: Use Enum to display the system password policy.

Also we can get the list of shares on the victim's computer.

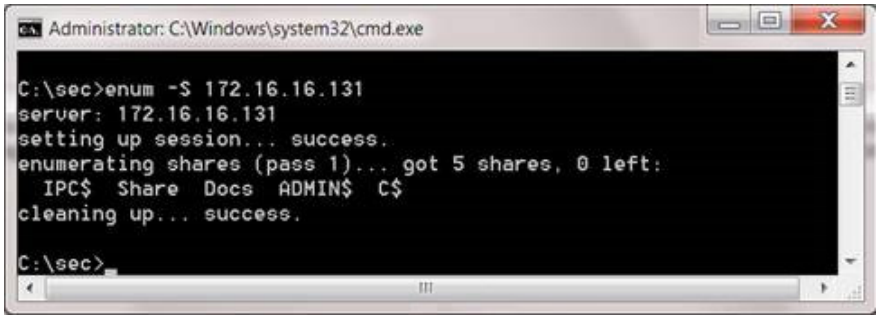

Figure 5: Use Enum to display shares on a system.

Enum provides a number of other options that can be used to get the same types of information, even integrating a basic lookup attack tool that helps cracking passwords based on user lists.

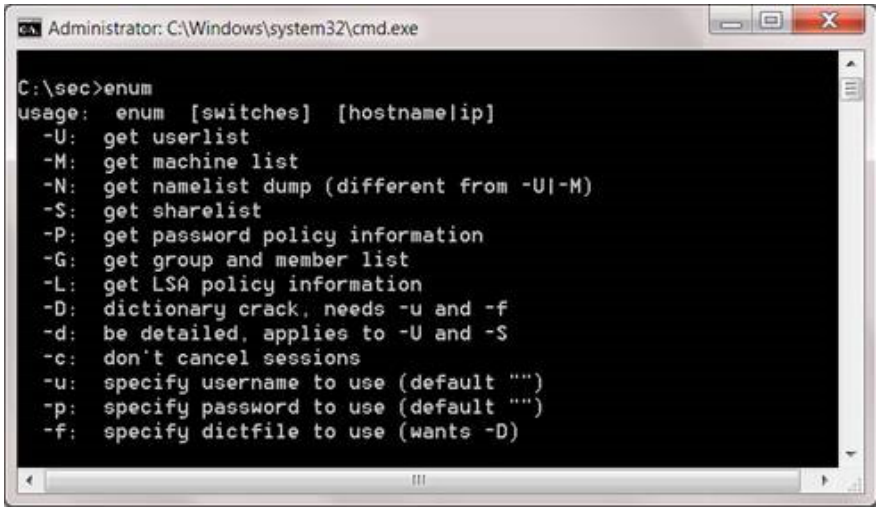

Figure 6: Enum's options list.

These options cannot retrieve the login information correctly, but this is a stepping stone and a key component for hackers to gain access to the victim's computer.

Null Session defense method

When thinking of hackers and attacks, perhaps the first question that is often thought of is 'does our system have weaknesses?' The answer depends on the operating system on the network environment. If you are running Windows XP, Windows Server 2003 or Windows 2000, the answer is 'yes' to some extent. This form of attack is difficult to do when users use higher operating system versions, but Windows XP and Windows Server 2003 are still the most popular operating systems. There are several other methods we can do to block null sessions.

Block null sessions in the registry

The compatibility of legitimate software and the fact that most businesses have to stick with old operating systems to tighten budgets are the two main reasons why Windows 2000 workstations and servers still exist. If you still use Windows 2000, you only need to make a small change in the Registry to block the ability to get information using null sessions.

When accessing **Regedit** and browsing to ***HKLM / System / CurrentControlSet / Control / LSA / RestrictAnonymous key*** , you can configure 3 options including:

1. 0 - Default setting. Unlimited access to null sessions.
2. 1 - Not only eliminates null sessions but also blocks the display of user names and shares.
3. 2 - Eliminate all values ??to null sessions by blocking all access.

As we can see, null sessions cannot be completely removed; however, its accessibility will be limited if you choose the installation option of 2. Be cautious when configuring this option on the server. Windows 2000 can

damage Clustering.

On Windows XP and Windows Server 2003, we can perform the same task in three Registry Keys:

HKLMSystemCurrentControlSetControlLsaRestrictAnonymous

1. 0 - Default setting. Null sessions can be used to list shares.
2. 1 - Null Session cannot list shares.

HKLMSystemCurrentControlSetControlLsaRestrictAnonymousSAM

1. 0 - null sessions can list users.
2. 1 - Default setting. Null sessions cannot list user lists.

HKLMSystemCurrentControlSetControlLsaEveryoneIncludesAnonymous

1. 0 - Default setting. Null sessions are not granted privileges.
2. 1 - Null sessions are considered part of the user group (quite dangerous and can allow shared access).

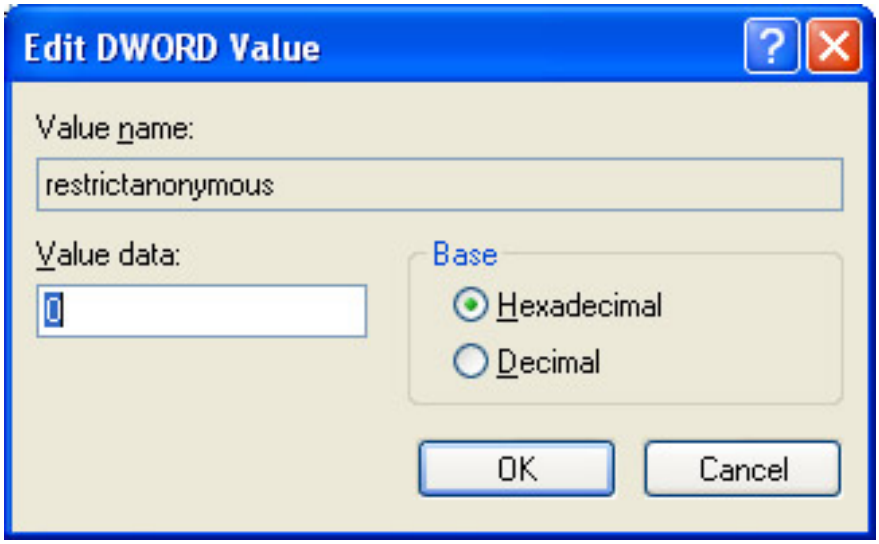

Figure 7: Modifying the RestrictAnonymous key in the Registry.

In Figure 7, by default Windows XP only allows to list the shares by default. This is a more secure setting than the same installation in Windows 2000, but it still provides information for an intruder.

Block access at network level

If you cannot make the changes in the Registry Keys mentioned above, then you can block all access with Windows Firewall or Network Firewall. This process can be done by blocking access to ports related to NetBIOS and SMB via TCP / IP. These ports include:

1. TCP port 135.
2. Port UDP 137.

3. UDP port 138.
4. UDP port 139.
5. TCP and UDP ports 445.

These ports are used for all networking functions of Windows, including File sharing, network printing, Clustering, and remote administration.

Note: *The process of blocking access to ports should be considered carefully before executing on multiple ports.*

Identify null sessions with IDS

If the Registry or Firewall changes remove the functionality of network applications, we must use a different method. Instead of blocking statistics through null sessions, one of the most effective measures is to discover null sessions as soon as possible to implement timely remedies such as when implementing a security event. normal network secret.

If you are using Snort, the most popular network IDS / IPS currently in a production environment, the following rule will detect Null Session statistics:

> **alert tcp $ EXTERNAL_NET any -> $ HOME_NET 139 (msg: 'NETBIOS NT NULL session'; flow: to_server.establshed;**
>
> **content: '| 00 00 00 00 57 00 69 00 6E 00 64 00 6F 00 77 00 73 00 20 00 4E 00 54 00 20 00 31 00 33 00 38 00 31 |'; classtype: attempted-recon;)**

This rule will not prevent null sessions, but it will notify you when a null session occurs.

Conclude

The null session concept is not a new threat, but it is always forgotten and overlooked. Using a null session attack, hackers can get information from the system. Understanding how to run null sessions is a must for those who are responsible for the security of systems on the network.

You finished reading the article "**Learn Null Session attacks**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.