Determine whether the system is compromised

In this article we will show you some methods to discover if someone is illegally tampering with your system.

Network Management - In this article we will show you some methods to discover if someone is illegally tampering with your system.

One of the biggest concerns for system administrators is compromise. This is the type of state that is illegally compromised by someone you don't know. Although it is only an unclear warning of antivirus software or a strange firewall message, it is best to perform an immediate or immediate check. In this article, I will show you some problems to find out if someone is illegally interfering with your system.

List open connections

One of the simplest and most effective ways you can do this is to list a list of open connections for your system. This can be done using the **netstat** command-line tool, which is available on both Linux and Windows operating systems. You can use netstat on Windows to list the list of listening TCP and UDP ports using the command ' *netstat -na* '. The output will show you four columns. The first column is the protocol in use (TCP or UDP), then the address and the local port, the third column is the address and the external port, and the last column is the state of the connection. Alternatively, you can use the ' *netstat -nao* ' *command* on newer Windows versions to get the fifth column showing the process ID associated with the displayed connections. An example of listing such connections is shown in Figure 1.

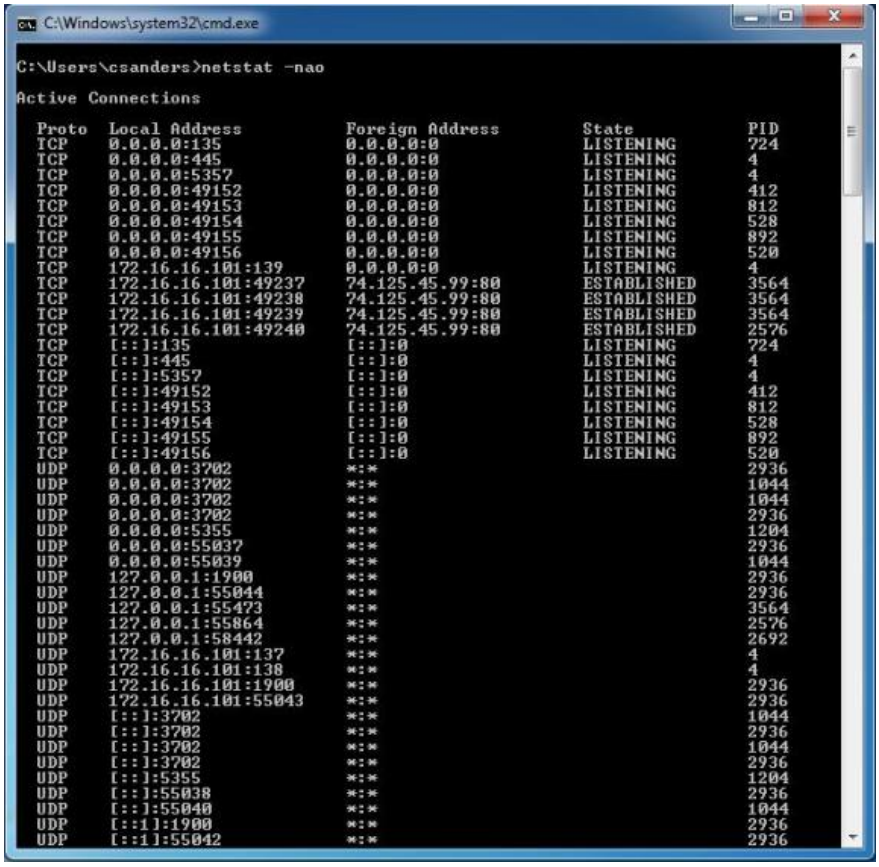

Figure 1: Output of *netstat -nao* command

When looking at netstat output you will probably be flooded with information. To avoid that, central network applications and processes need to be closed to reduce clutter. After doing that, the first thing you should look for here is unrecognized external addresses, especially in ESTABLISHED status. In addition, it is also necessary to search for LISTENING connections on the local system on the old ports. When an attacker compromises the system, they will usually leave a backdoor that can then listen to the connections more easily. Based on that sign, we can know the connections in our system.

One important thing to note here is that netstat can still make mistakes. For example, in case of kernel-mode rootkits can be used by an attacker to change netstat and hide the backdoor they install.

Check the line

Suppose if someone is controlling your system, one thing is that they must access your network via a network card. With that in mind and a problem like the one above that netstat does not have to be 100% accurate, we need to use another method of using packet inspection applications. Through such applications, we can check the data packets in the transmission environment (wired or radio waves).

To 'sniff' data packets quickly, you can use **Wireshark** software, which is the most popular data sniffing app in the world today. The application is easy to install and use, open source (free) and has a graphical interface. If you like using the command line you can also use the command line tool component of Wireshark, Tshark, or even more popular than Windump. Windump is also a free application and works quite well. Using any method, you can capture packets transmitted through the network interface and find IP addresses that appear outside the

system.

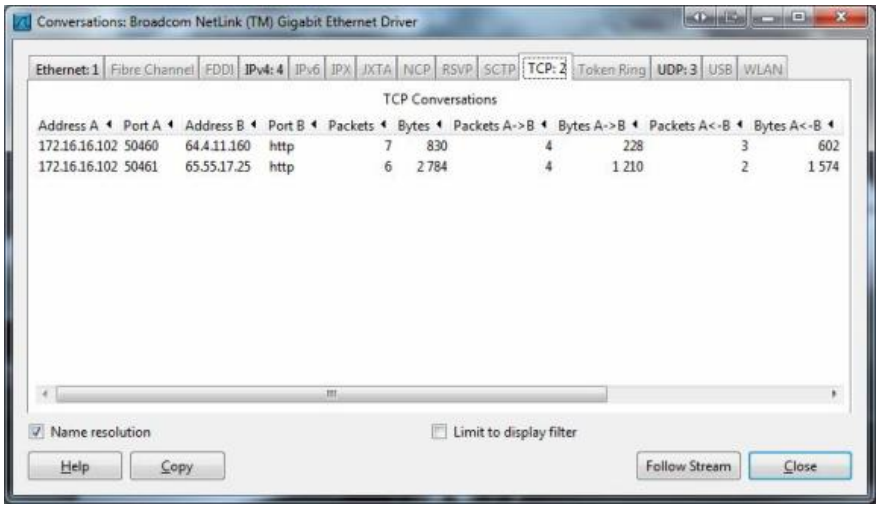

Figure 2: Use Wireshark to check the conversation

One problem to mention here is that when checking data packets, services that are using the network should be turned off to avoid confusion in the results. You can observe the conversations that appear between your system and the outside world by selecting the **Statistics** option from the drop-down menu and clicking **Conversations** . This window allows you to see the active communication hosts categorized in different ways, as shown in Figure 2.

Check the log files

Log files are also one of the essential things for network administrators, software experts and intrusion analysts. The quickest way to access the event view on your Windows system is to type ' *eventvwr.msc* ' from the 'Run' dialog box or the command line. From here you can check all the records to compare the conflict with your daily activities. Some of the events we look for include:

1. Large number of login attempts failed. This indicates that if someone tries to guess or perform a *brute force* attack on the account password.
2. The event log service is being stopped. This often indicates that the attacker has turned off this service as soon as the system is compromised to remove the trace.
3. Unusual services appear. Any service that you don't feel confident about can be considered malicious.

Use Process Monitor to check the Registry and running processes

The two most important areas to observe when trying to determine whether a system is compromised are not the system registry and running processes. Any changes to the system are reflected in the registry and every task that appears on a system is done with a certain process. Previously, testing such things was complicated, but today we have the support of the Process Monitor tool of Windows Sysinternals. Using the Process Monitor tool you can see changes to the registry as they occur and see the active processes and details related to them. To get this software you can download it here.

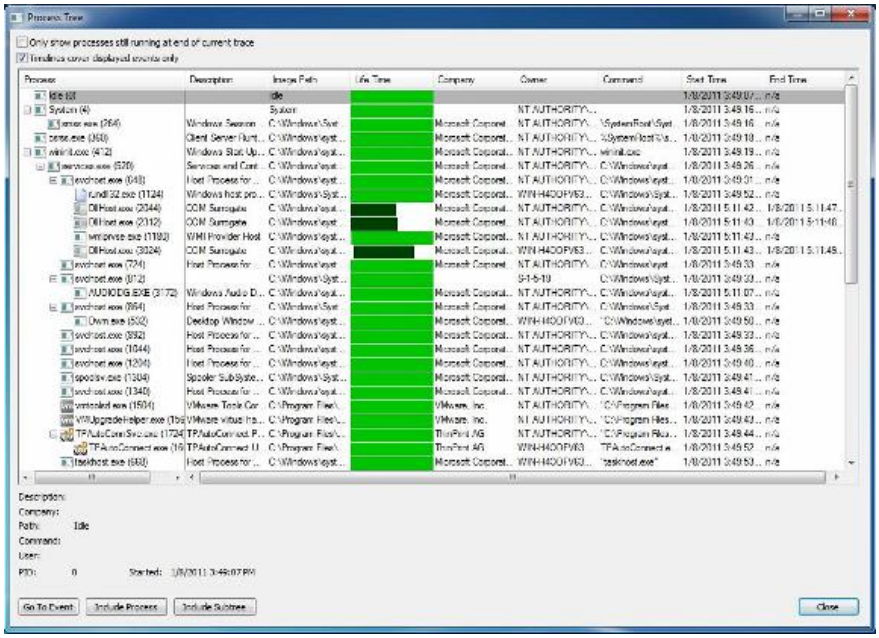

Figure 3: Viewing processes in the tree view of a test set

To be able to analyze the registry and running processes requires you to have some basic knowledge. If you run the test regularly, you will easily know which processes are normal and which processes are malicious.

Check user accounts

The last one may be too simple, but it still needs to be listed here to check the user accounts on your system. Many times when an attacker compromises your system has created a new user account to easily access your system next time. To perform a test, go to the **Start** menu and right-click **Computer** , right-click **Manage** , browse to **Users and Groups** .

Conclude

In this article we have provided you with some basic knowledge about whether or not the system is compromised. And one thing we need to know is that proactive security is always the best way to protect the system against attacks.

Some reference commands: http://www.sans.org/security-resources/winsacheatsheet.pdf