DATACOM
SYSTEMS INC

Network Tap Tutorial

The concept of electronic wiretapping goes back to the early years of the telegraph. Information was sent through the telegraph line, such as the codes of safes being shipped, and the trains personal safe code. Bandits would tap into the line, decode the information and then just show up at the train depot, show that they had received the telegraph, open the various safes and take take everything.

Overview

The ability to collect and understand traffic in a computer network has long been the object of many IT manager's desires, dreams and nightmares. Many companies have created hardware and software to detect, analyze and report utilization, protocols and baselines. As these tools and their reporting have improved over time, the method they use to capture data has remained relatively unchanged. The Test Access Point or TAP provides network analysis and security tools access to network communications undetected.

History

The concept of electronic wiretapping goes back to the early years of the telegraph. Information was sent through the telegraph line, such as the codes of safes being shipped and the trains personal safe code. Bandits would tap into the line, decode the information and then just show up at the Train depot and walk in show them that they had received the telegraph and could open the safes, and they would just take everything.

In this century a wiretapping case eventually made it to the United States Supreme Court.

Olmstead v. United States, the first wiretapping case in Supreme Court history, unfolded within the context of Prohibition, eight years after the Eighteenth Amendment, which barred the sale, distribution and consumption of alcoholic beverages, passed into law. Olmstead, a bootlegger, had been convicted largely on evidence gathered via a wiretap that law enforcement officials placed on the telephone in his place of business.

Olmstead argued that the wiretap amounted to an illegal search and, therefore, violated his rights under the Fourth Amendment, the Court ruled that electronic eavesdropping did not violate protections against illegal search because it did not involve physical entry.

According to the Court, Olmstead had, in effect, broadcast his conversations to the general public whenever he spoke on the phone. According to Justice Taft, who wrote the majority opinion, "The language of the amendment cannot be extended and expanded to include telephone wires, reaching to the whole world from the defendant's house or office. The intervening wires are not part of his house or office, any more than are the highways along which they are stretched."

Network Tap Tutorial

Development

Early taps were used to collect information on high availability or critical links, without breaking the connection. These connections that were of greatest interest were typically on the edge of a companies network. The edge device connects to another company, known as the service provider. The service provider offers wide area connectivity to the company network, to give them availability into the internet, or into a private network between corporate offices.

Network taps are frequently used around firewalls, but can be used on any network connection.

Conventional Tap

The simplest form of tap, is the conventional tap or non-aggregating tap. A conventional tap passes traffic between two devices (i.e. A and B) and has two output monitor ports. The first monitor port sends out the copy of traffic going from device A to device B. The second monitor port sends out the copy of traffic going from device B to device A.

The benefit of a conventional tap is that there is no contention on the output monitor ports. A full-duplex 1 Gbps connection between two network devices can potentially produce 1Gbps in each direction. This yields a total of 2Gbps on the link, or 1Gbps in each direction. The two output monitor ports from the tap each carry a full 1Gbps.

Many inexpensive or opensource network analysis tools use just one network interface cards (NIC).

In order to use a network analysis tool with a single NIC you can only listen to one side of the conversation at a time, if a conventional tap is in use.

There are dual NIC analysis tools available, but they need to merge the two traffic streams together to produce a single trace file that allows the analyst to see the entire conversation.

Active vs. Passive

An active tap reroutes network traffic into the taps inner electronics, makes a copy, then sends the traffic on to its destination. The copy gets sent to the monitoring device(s). Active taps are susceptible to power outages, since they use the devices internal electronics to route traffic.

An active tap would reroute traffic from device A, while making a copy of the traffic, and send the traffic on to device B. During this process the copy of the traffic is sent out the monitor ports.

A passive tap passes all data packets, even during a power outage. between network devices.   Note that during a power outage, or tap electronic equipment failure, the monitoring device off the tap may not receive data. However, a truly passive tap will always pass data between network locations.

Benefits

Taps are permanent access points which provide security and analysis personnel network visibility. They provide permanent access for devices to be connected for monitoring and security purposes. Many tap models can see traffic from all seven layers of the OSI model, and do not have MAC addresses so are invisible to the network. Conventional taps pass line rate, non-aggregated traffic. Most taps come with redundant power supplies.   Use passive taps to always pass 100% of the traffic between network devices, even in the event of a power loss to the tap.

No coordination with ISPs or network departments is required to use a conventional tap. The monitor ports are always on and available for network analysis.

Since taps are a permanent, invisible device, no network configuration changes are required to gain access to network traffic. Taps do not place any additional load on network devices and the use of a tap does not consume any ports on routers or switches.

Drawbacks

Taps must be inserted into the network, which requires scheduled down time, and typically require power. For security purposes, they should be in a locked area or facility.

Analysis tools using a non-aggregation tap, are required to have dual NICs if both sides of a network conversation need to be on a single trace file. A single NIC tool can be used, but only one side of the conversation can be see at a time.

Conclusion

Taps are a critical part of any complex communications infrastructure. They provide security and analysis personnel improved access for monitoring specific network segments, without increasing load on network devices or requiring any reconfiguration of network components.

For more information, visit

www.datacomsystems.com

DATACOM
SYSTEMS INC