Packet Sniffing

Hao Huang

INTRODUCTION:

It is a crucial issue when people are talking about the information security via the network. It's packet sniffing. I have to say that packet sniffing is like a double-edge sword. It could be used by many network technicians, engineers to detect network faults, monitor and troubleshoot daily network traffic to maintain network flows efficient. However, it also could be used to do bad things via capturing data passing through the network by some packet analyzers. We can avoid the fact that there are people doing this without our attentions. Follow an old saying in China: know your enemy and know yourself, so this project's main goal is to explore how exactly packet sniffing works and how to detect network intrusion attempts to protect our information, all of those this project is going to talk about would tell us how important to securing or encrypting our data is.

BACKGROUND THEORY:

Packet sniffing is a technique of monitoring every packet that crosses the network. It can be done on both wired broadcast LANs and wireless LANS via particular packet sniffers. Because IP makes no effort to validate whether the source address in the packet generated by a node is actually the source address of the node, you can spoof the source address and the receiver will think the packet is coming from that spoofed address.

As for a wired LAN, all clients are being connected together with a hub or a switch. So they can communicate with each other in this little LAN directly. One very important point to understand here is the packet sniffer need to be on the same wired LAN. In another way, our probing devices should be deployed on the same wire which clients are using to communicate with.

Basically, there are three different sniffing:

IP-based sniffing:

This is the original way of packet sniffing. It works by putting the network card into promiscuous mode and sniffing all packets matching the IP address filter. Normally, the IP address filter isn't set so it can capture all the packets. This method only works in non-switched networks.

MAC-based sniffing:

This method works by putting the network card into promiscuous mode and sniffing all packets matching the MAC address filter.

ARP-based sniffing:

It doesn’t put the network card into promiscuous mode but to poison the ARP caches of the two hosts that you want to sniff first. The most important thing is identifying you as the other host in the connection. Once the ARP caches are poisoned, the two hosts start their connection, but instead of sending the traffic directly to the other host it gets sent to us. We then log the traffic and forward it to the real intended host on the other side of the connection. This is called a man-in-the-middle attack.

To make it clear, we set a situation where clients A, B, C, D are being connected with a central device such as a switch or hub to explain more about ARP. Client A wants to send messages to client D and client B attempts to sniff these messages. So a packet sniffer is installed on client B. Here we just consider packet sniffer as software using which we can capture and sniff data, deep discussion about packet sniffer would come next.

As for a WLAN, it is becoming easier than wired ones. There is no need to find a way to install a sniffer on one or more of the hosts in the targeted subnet.

Wireless Overview:

In an infrastructure WLAN, stations connect to each other via airwave with an access point, aka AP, which accepts wireless signals from multiple nodes and retransmits them to the rest of the network. As long as a station is on and has its wireless protocols running, it periodically surveys its surroundings for evidence of an access point, a task known as scanning. It may use either active scanning or passive scanning. In active scanning, the station transmits a special frame, known as a probe, on all available channels within its frequency range. When an access point finds the probe frame, it issues a probe response. [1] This response contains all the information a station needs to associate with the access point. After receiving the probe response, a station can agree to associate with that access point. The two nodes begin communicating over the frequency channel specified by the access point.

Association:

Data can be exchanged between the station and AP only after a station is associated with an AP in the infrastructure mode or with another station in the ad hoc mode. All the APs transmit Beacon frames a few times each second that contain the SSID, time, capabilities, supported rates, and other information. [1] Stations can chose to associate with an AP based on the signal strength etc. of each AP. Stations can have a null SSID that is considered to match all SSIDs.

The association is a two-step process. A station that is currently unauthenticated and unassociated listens for Beacon frames. The station selects a BSS to join. The station and the AP mutually authenticate themselves by exchanging Authentication management frames. The client is now authenticated, but unassociated. In the second step, the station sends an Association Request frame, to which the AP responds with an Association Response frame that includes an Association ID to the station. The station is now authenticated and associated.

A station can be authenticated with several APs at the same time, but associated with at most one AP at any time. Association implies authentication. There is no state where a station is associated but not authenticated.

METHODOLOGY:

ARP Poisoning:

As its name standing for Address Resolution Protocol, we use ARP to match IP address to its MAC address. According to the ARP, it normally works whenever client A initiates a connection to client B with B's IP address, client A first looks up its own ARP cache to see if there already has a MAC address matching that IP address. If there has one, client A would use that MAC address as Target Hardware Address. If there hasn't, A would broadcast the ARP request to see if any other else in this LAN has an identical IP address, then that client would unicast a ARP reply back with its MAC address. After the ARP message has been composed it is passed down to the data link layer for transmission. However, the ARP does not provide for any verification for the ARP replies. So crackers exploit this lack by "poisoning" A's ARP. Here client B accomplishes this by sending an ARP Reply packet that is deliberately constructed with a "wrong" MAC address to client A. The ARP is a stateless protocol. Thus, A receiving an ARP Reply cannot determine if the response is due to its request it sent or not. Consequently, client B would receive the messages which were intended to be sent to client D from client A.
Don't forget to enable "ip_forwarding" on the attacking machine otherwise it would break down traffic between 2 machines

Passive Scanning:

Scanning is the act of sniffing by tuning to various radio channels of the devices.
A passive network scanner instructs the wireless card to listen to each channel for a few messages. This does not reveal the presence of the scanner. [1]
An attacker can passively scan without transmitting at all. Several modes of a station permit this. There is a mode called RF monitor mode that allows every frame appearing on a channel to be copied as the radio of the station tunes to various channels. This is analogous to placing a wired Ethernet card in promiscuous mode. This mode is not enabled by default. [4] Some wireless cards on the market today have disabled this feature in the default firmware. One can buy wireless cards whose firmware and corresponding driver software together permit reading of all raw 802.11 frames. A station in monitor mode can capture packets without associating with an AP or ad-hoc network. The so-called promiscuous mode allows the capture of all wireless packets of an associated network. In this mode, packets cannot be read until authentication and association are completed.

Man-in-the-Middle Attack:

Man-in-the-middle (MITM) attack refers to the situation, but in a wireless circumstance, where an attacker on client B inserts itself between all communications between clients A and D, and neither A nor D is aware of the presence of B. All messages sent by A do reach D but via B, and vice versa. The attacker can merely observe the communication or modify it before sending it out. An MITM attack can break connections that are otherwise secure. At the TCP level, SSH and VPN, e.g., are prone to this attack. [2]
Assume that station A was authenticated with D, a legitimate AP. Attacker B is a laptop with two wireless cards. Through one card, he will present himself as an AP. Attacker B sends de-authentication frames to A using the D's MAC address as the source, and the BSSID he has collected. A gets de-authenticated and begins a scan for an AP and may find B on a channel different from D. There is a race condition between B and D. If A associates with B, the MITM attack succeeded. B will re-transmit the frames it receives from A to D, and the frames it receives from D to A after suitable modifications.

DETECTION AND SECURE PRACTICES:

It has been revealing that there are highly possibilities to expose our information. To make it worse, many services on the internet send data in the plain text. By default, POP mail, SMTP send data all in clear text. The same applies for FTP, Telnet and even MSN. In fact most services send passwords this way.

Switch Network:

To low the risk, both in wired situations or wireless circumstance, using a switch rather than a hub can enhance the security. In the non-switched environment, packets are visible to every node on the network, in a switched environment; packets are only delivered to the target address. Unlike hubs, switches only send frames to the designated recipient; therefore a NIC in promiscuous mode on a switched network will not easily capture every piece of local traffic. This provides extremely efficient protection in practice because it takes more work to successfully sniff. [3]

Anti-Sniffing Tools:

A scary aspect of these tools is who can, and will, use them. As stated earlier, sniffers can be used for both legitimate and illegitimate purposes. Defending against sniffers, as with any other threat, needs to start from the top and filter down to the user. As on any network, administrators need to secure individual machines and servers. A sniffer is one of the first things a cracker will load to see what is taking place on and around their newly compromised machine.
Another method of protection involves tools, such as anti-sniff, that scan networks to determine if any NICs are running in promiscuous mode. These detection tools should run regularly, since they act as an alarm of sorts, triggered by evidence of a sniffer.

Encryption:

As far as I know, encryption is the best protection against any form of traffic intrusion. The easiest way to protect your password is to use uncommon characters. In addition, the ways below would provide us a secure practice:

1. When logging into to mail services check to see if your mail client supports encrypted login's. The server has to support this setting too, so check with them.
2. Even if you login securely (above) any e-mail you send is still in clear text, anyone on the path that the mail travels through can technically read it. Use Encryption to encrypt the message. PGP (www.pgpi.org) is the popular application for this
3. When shopping on-line make sure the store has a "secure" connection for submitting credit card details. Generally SSL 128bit encryption is the standard.
4. Telnet sends password and normal data in plain text. If your server supports SSH then use this instead of Telnet since the connection is encrypted.[5]

CONCLUSION:

Having looked at what Packet Sniffing is, why it works and how it is used, it is easy to tell it as both dangerous threat and powerful tool. Every user should understand they are vulnerable to these types of attacks and their best defense lies in details. Also, Administrators and professionals need to know that it is a superb diagnostic method that can, unfortunately, be used with malicious intent on any network. [5]

REFERENCES:

[1]Tamara Dean, "Network__Guide_to_Networks__5th_Edition", 2010

[2]"IP Spoofing an Introduction," http://www.securityfocus.com/infocus/1674

[3]Manu Garg, "Sniffing in a Switched Network --With A Recipe To Hack A Switch Using

Ettercap and Ethereal"

[4]http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_10-4/104_ip-spoofing.html

[5] http://www.symantec.com/connect/articles/sniffers-what-they-are-and-how-protect-yourself