1 Sniffen

1.1 Erklärung

Ein Sniffer (von „to sniff“ = schnüffeln) ist ein Werkzeug der LAN-Analyse. Dabei handelt es sich um eine Software, die den Datenverkehr im Netzwerk lauschen, aufzeichnen und darstellen kann. Der Begriff „Sniffer“ bezeichnete ursprünglich ein LAN-Analysetool der Firma Networks General. Da dieses Produkt eines der Ersten auf dem Markt und am weitesten verbreitet war, hat sich der Name allgemein durchgesetzt für die Bezeichnung von LAN-Analysetools.

1.2 Anwendung

Sniffer werden für folgende Zwecke eingesetzt:

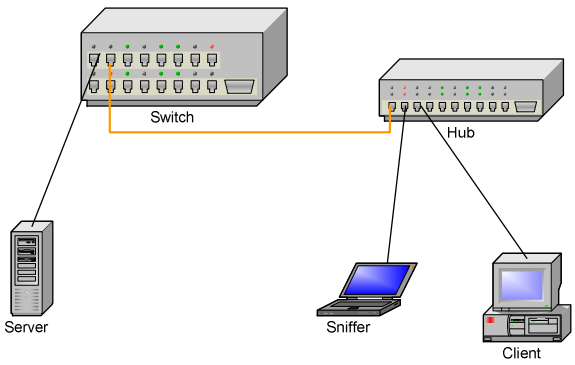
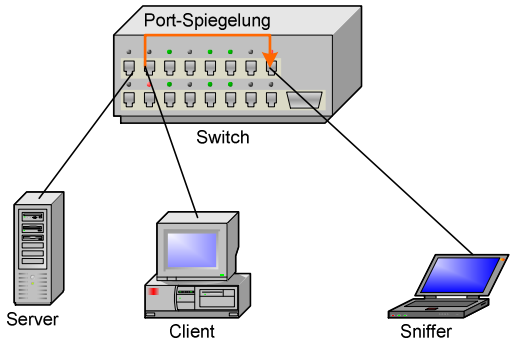
- Diagnose von Netzwerkproblemen
- Eindringungsversuche entdecken
- Netzwerk-Traffic-Analyse nach verdächtigem Inhalt
- Datenspionage / Hacken

Ein Sniffer kennt zwei verschiedene Sniff-Modi:

1. **Non-Promiscuous Mode:**
   In diesem Modus wird der eingehende und ausgehende Datenverkehr des eigenen Computers gesnifft.

2. **Promiscuous Mode:**
   In diesem Modues sammelt der Sniffer den gesamten Datenverkehr der Netzwerkschnittstelle oder den Datenverkehr eines definierten Bereichs. Es werden nicht nur die an ihn adressierten Frames mitgehört, sondern auch die nicht an ihn adressierten. Der Adressat eines Frames wird im Ethernet-Netzwerk durch seine MAC-Adresse identifiziert.

In heutigen „geswitchten“ Netzen wird man feststellen, dass man nicht sehen kann, wie zwei andere Clients miteinander kommunizieren. Dies ist so, weil der Switch die ankommenden Datenpakete nur an den in der „Switching Table“ eingetragenen Port der Zieladresse weiterleitet. Man kann also nur den eigenen Datenverkehr und Broadcasts sehen.
Um den Netzwerkverkehr zwischen anderen Clients zu betrachten, gibt es folgende Lösungsmöglichkeiten:

Schaltung über einen Hub	**Port Spiegelung auf dem Switch**
	
Hier spielt die Tatsache, dass Hubs alles (Uni-, Multi- & Broadcasts) an alle Ports weiterleiten, eine wichtige Rolle. Der Hub wird am Switch angeschlossen. Der Client wird nun zusammen mit dem Sniffer an einen Port des Hubs angeschlossen. Der Sniffer kann nun den ganzen Netzwerkverkehr, der über den Hub geht, sniffen.	Diese Variante ist etwas bequemer und führt auch zu keinem Netzwerkunterbruch. Allerdings wird Port-Spiegelung nicht von jedem Switch unterstützt. Dem Sniffer-Port wird gesagt, dass er den Client-Port „monitoren“ soll. Nun wird der gesamte Netzwerkverkehr dieses Ports auf den Sniffer-Port kopiert und der Sniffer kann nun den Traffic sehen.

1.3 Sniffertools

1.3.1 Freeware

- Wireshark (ehemals Ethereal)
- Packetyzer
- Tcpdump
- Ettercap

1.3.2 Lizenzpflichtig

- Sniffer (Network General)
- OptiView (Fluke Networks)
- EtherPeek, OptiPeel, GigaPeek (WildPackets)
- LANdecoder32 (Triticom)

2 Quellenangaben

2.1 Internet

benötigt für:	Link:
Sniffer	http://de.wikipedia.org/wiki/Sniffer