Packetsniffing

Übersicht

- Was ist Packetsniffing überhaupt?
- Wie funktioniert Packetsniffing?
  - Das Programm Wireshark
  - Packetsniffing Beispiel HTTP-GET Request
- Wozu wird es benutzt?
- Fazit

Was ist Packetsniffing überhaupt?

- Netzwerkanalyse
  - Prüfung eines Kommunikationsnetzes
- Packetsniffing
  - Eine mögliche Art von Netzwerkanalyse
  - Datenverkehr wird aufgezeichnet, jedes Paket wird einzeln analysiert

Wie funktioniert Packetsniffing?

- Mit Hilfe von sogenannten Packet Sniffern
- Hardware- oder Softwarerealisierungen
- Hardware Sniffer heutzutage kaum noch gebräuchlich
- Packet Sniffer wird an benötigter Stelle innerhalb des Netzwerks eingesetzt

Das Programm Wireshark

- Open Source Programm zur Netzwerkanalyse
- Hieß früher „Ethereal“
- Aktuelle Versionsnummer 1.11.1
- Am weit verbeitetes Werkzeug für Netzwerkanalyse
- Software Sniffer

Packetsniffing Beispiel HTTP-GET Request

Live-Demonstration

Wozu wird es benutzt?

- Diagnose
  - Netzwerkfehler finden
- Optimierung
  - Bandbreitenauslastung analysieren
  - Effizienteste Paketgröße bestimmen
- Sicherheit
  - Paketwege analysieren
  - Datenverkehr speichern als späteres Beweismittel
- Angriff
  - Datenspionage

Fazit

- Ist Packetsniffing für die Sicherheit in einem System zu gebrauchen?
- Eindringlinge sind schwer zu erkennen
- Paketanalyse wird mit mehr Daten aufwändiger
- Gesammelte Daten verbrauchen viel Speicherplatz

Genutzte Literatur

- Laura CHAPPELL. Wireshark network analysis. 1. Auflage. San Jose:Chappell Univ., 2010.
- Chris SANDERS. Practical Packet Analysis : using Wireshark to solve real-world network problems. 2. Auflage. San Francisco, CA: No Starch Press, 2011.
- Wikipedia. URL: http://de.wikipedia.org/wiki/Wireshark.