Netzüberwachung / - Spionage

Spezial-Hardware und Bordmittel

Vorlesung Netzwerk/Sicherheitsmanagement

Ralph Niederberger
r.niederberger@fz-juelich.de
08.12.2003

Sniffer

Gerät, dass an Computernetze angeschlossen wird, den Datenverkehr analysiert und lesbar macht

Je nach Netzwerkstruktur ist beliebiger Verkehr mitlesbar (shared medium)

Nicht möglich in strukturierter Verkabelung (switch medium)

Gerät benutzt promiscuous mode

mehrere Arten:

- kommerzielle Packet Sniffer
- kommerzielle/public Domain Software
- underground packet sniffer

Sniffer Nutzung

- Automatische Suche nach Klartext-Passwörtern
- Konversion von Daten in lesbare Form
- Fehleranalyse zur Netzwerkproblemlösung
- Performance-Analyse bei Bottlenecks
- Network Intrusion Detection (Discover)
- Network Traffic Logging (Prevention)

Sniffer Komponenten

- Hardware
- Capture Driver
  - Filtert Verkehr am Interface entsprechend der eingestellten Parameter und liefert ihn am Buffer ab
- Buffer
  - Speicherung, solange noch Platz oder Round Robin
- Echtzeitanalyse
  - Suche nach Fehlern, Netzaus-/überlast, Hackeraktivität, ...
- Decodierung
  - Ausgabe in lesbarer Form
- Packet Editing/Transmission
  - Wiedereinspielen gleicher/geänderter Packete

Switched Network Sniffing

- Switch Jamming (Überfluten der Mac Tabelle)
- ARP Redirect (Aussenden falscher ARP-Responses)
- ICMP Redirect (Mitteilung über angeblich fasche Route)
- ICMP Router Advertisement (Mitteilung, wer Router ist)
- MAC-Adresse des Ziels übernehmen (Router irreführen)
- Umkonfiguration des Span/Monitor-Ports
- Cable-Taps (Abhören des Kabels)

Sniffer-Arten

- Distributed Sniffer

  besteht aus
  - Management-Station(s) (mit GUI) Hardware &/oder Software
  - Sniffer Appliances verteilt im Netz (Hardware &/oder Software)
- Portable Sniffer
  - Tragbares Gerät, dass an die zu untersuchende Stelle im Netz angeschlossen wird. Flexibel einsetzbar bei Problem-Verdacht
  - Auch hier: Hardware &/oder Software
- Wireless Sniffer
  - Gerät zum Sniffern von Funknetzen, inklusive Erkennung illegaler Maschinen und Accesspoints, Wep-Decryption, ...

*[1] Sniffer Trademark von Network Associates

tcpdump (Linux)

tcpdump - dump traffic on a network

Syntax: /usr/etc/tcpdump [-deflnNOpqStvx]
[-c count] [-F file] [-i interface]
[-r file] [-s snaplen] [-w file] expression

Description

The tcpdump command prints out the headers of packets on a network interface that match the specified boolean expression.

Under SunOS: You must be root to invoke tcpdump or it must be installed setuid to root.

Under ULTRIX: Any user can invoke tcpdump once the super-user has enabled promiscuous-mode operation using pfconfig(8c).

Under BSD: Access is controlled by the permissions on /dev/bpfn, where n is the unit number of the device.

Options .....

tcpdump (2)

tcpdump -xvv -s 512 ip proto 'UDP' and port 53 and host dante

09:04:42.694 dante.1432 > zam048.domain: 18+ (53)(ttl 59, id 25336)

```
4500 0051 62f8 0000 3b11 65da 865e 5354
865e 5002 0598 0035 003d 0000 0012 0100
0001 0000 0000 0000 067a 616d 3030 3103
7a61 6d09 6e61 6d65 2074 656d 700b 6b66
612d 6a75 656c 6963 6802 6465 0000 0100
01
```

4500 0051 62f8 0000 3b11 65da 865e 5354
Vers4 Headlen5 ServType00 TotalLen0051=81 Ident62F8
FlagsFragOffSet0000 TTL3B=59 Prot11=UDP
HeadCheckSum65DA Source865E5354=134.94.83.84
865e 5002 0598 0035 003d 0000 0012 0100
Dest865E5002=134.94.80.2 ||||UDP-Paket SoucePort0598=1432
DestPort0035=53 UDPMessLen003D=61 UDPCheckSum0000
||||DATA-DNS-Paket Ident0012 Param0100
Param0100=00000001 00000000=
0Query 0000Standard 0NonAuth 0NotTrunc
1RecursionDesired 0RecursionAvailable
000Reserved 0000NoError
0001 0000 0000 0000 067a 616d 3030 3103
#ofQuest0001=1 #ofAnsw0000=0 #ofAuth=0000=0 #ofAddit0000=0
||||QuestionSection ||||QueryDomName Len06=6
7a616d303031=zam001 Len03=3
7a61 6d09 6e61 6d65 2074 656d 700b 6b66
7a616d=zam Len09=9 6e616d6520686c727a=name temp
Len0B=11 6b66=kf
612d 6a75 656c 6963 6802 6465 0000 0100
612d6a75656c696368=a-juelich Len02=2 6465=de EndofDomname00
QueryTyp0001 QueryClass0001
01
QueryClassSecByte01

tcpdump (3)

09:04:42.694 zam048.domain > dante.1432: 18 FormErr 0/0/0 (12)(ttl 30, id 45495)

4500 0028 b1b7 0000 1e11 3444 865e 5002
865e 5354 0035 0598 0014 c19a 0012 8181
0001 0000 0000 0000 0000 0000 0000

4500 0028 b1b7 0000 1e11 3444 865e 5002
Vers4 Headlen5=20Byte ServType00 TotalLen0028=40
IdentB1B7 FlagsFragOffSet0000 TTL1E=30 Prot11=UDP
HeadCheckSum3444 Source865E5002=134.94.80.2
865e 5354 0035 0598 0014 c19a 0012 8181
Dest865E5354=134.94.83.84 ||||UDP-Paket SoucePort0035=53
DestPort0598=1432 UDPMessLen0014=20 UDPCheckSumC19A
||||DATA-DNS-Paket Ident0012 Param8181
Param8181=10000001 10000001=
1Response 0000Standard 0NonAuth
0NotTrunc 1RecursionDesired
1RecursionAvailable 000Reserved
0001FormatError
0001 0000 0000 0000 0000 0000 0000
AnswerClass0001

tcpdump (4)

09:05:32.108 dante.1435 > zam048.domain: 21+ (43)(ttl 59, id 25436)

4500 0047 635c 0000 3b11 6580 865e 5354
865e 5002 059b 0035 0033 0000 0015 0100
0001 0000 0000 0000 067a 616d 3030 3103
7a61 6d0b 6b66 612d 6a75 656c 6963 6802
6465 0000 0100 01

4500 0047 635c 0000 3b11 6580 865e 5354
Vers4 Headlen5=20Byte ServType00 TotalLen0047=71
Ident635C FlagsFragOffSet0000 TTL3B=59 Prot11=UDP
HeadCheckSum6580 Source865E5354=134.94.83.84
865e 5002 059b 0035 0033 0000 0015 0100
Dest865E5002=134.94.80.2 ||||UDP-Paket
SoucePort059B=1435 DestPort0035=53
UDPMessLen0033=51 UDPCheckSum0000
||||DATA-DNS-Paket Ident0015 Param0100
Param0100=00000001 00000000=
0Query 0000Standard 0NonAuth
0NotTrunc 1RecursionDesired
0RecursionAvailable 000Reserved
0000NoError
0001 0000 0000 0000 067a 616d 3030 3103
#ofQuest0001=1 #ofAnsw0000=0
#ofAuth=0000=0
#ofAddit0000=0
||||QuestionSection ||||QueryDomName Len06=6
7a616d303031=zam001 Len03=3
7a61 6d0b 6b66 612d 6a75 656c 6963 6802
7a616d=zam Len0B=11
6b66612d6a75656c696368=kfa-juelich
Len02=2
6465 0000 0100 01
6465=de EndofDomname00 QueryTyp0001
QueryClass0001

iptrace (AIX)

Purpose:

Provides interface-level packet tracing for Internet protocols.

Syntax:

/usr/sbin/iptrace [-a] [-e] [-PProtocol] [-iInterface]
[-pPort] [-sHost [-b]] [-dHost [-b]] LogFile

Description:

The /usr/sbin/iptrace daemon records Internet packets received from configured interfaces. Command flags provide a filter so that the daemon traces only packets meeting specific criteria. The LogFile parameter specifies the name of a file to which the results of the iptrace command are sent.

snoop (SunOS/Solaris)

snoop - capture and inspect network packets

SYNOPSIS

snoop [-aqrCDNPSvV] [-t [r | a | d]] [-c max-count] [-d device] [-i filename] [-n filename] [-o filename] [-p first [, last]] [-s snaplen] [-x offset [, length]] [expression]

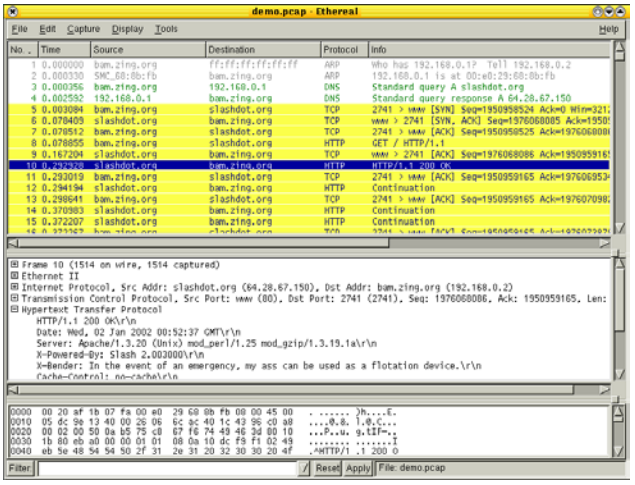
DESCRIPTION

snoop captures packets from the network and displays their contents. Captured packets can be displayed as they are received, or saved to a file for later inspection.

ethereal

- Frei verfügbares Netz-Analyse-Tool für Unix und Windows
- Ermöglicht Daten direkt vom Netz bzw. aus einer Datei zu untersuchen
- Interaktives GUI für Summary und Detail-Informationen für jedes Paket
- Möglichkeit einen TCP-Stream zu rekonstruieren

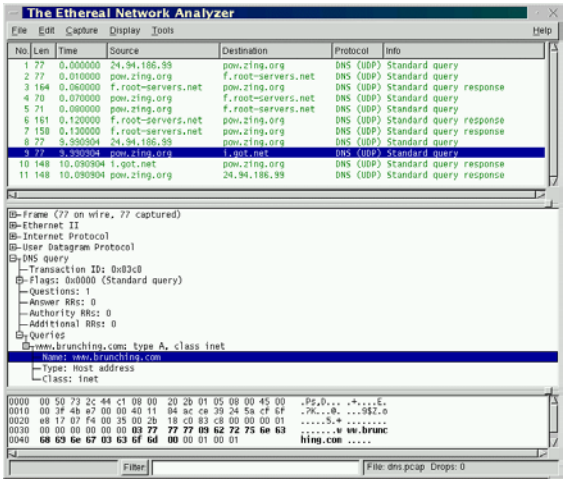
ethereal GUI



Hauptfenster

Listet die captured packets

ethereal GUI

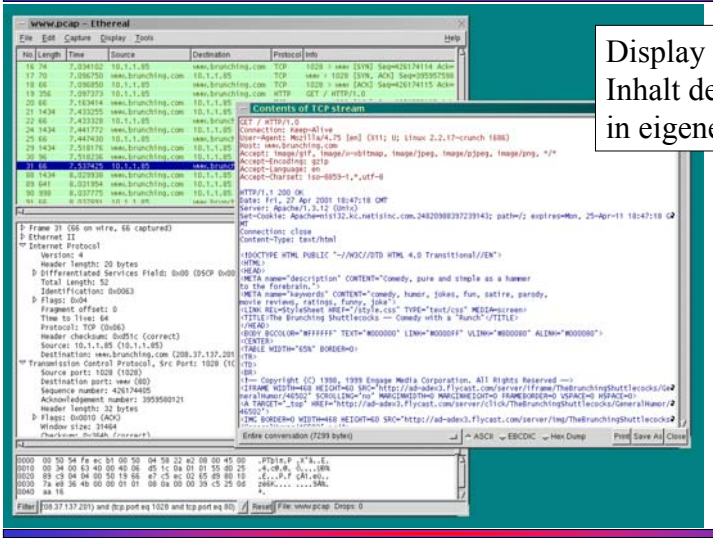


DNS-Anfrage aus Serversicht

Server macht rekursive Anfrage für den Clienten

Client fragt erneut, bevor er Antwort bekommt

ethereal GUI



Display ASCII Inhalt des Paketes in eigenem Fenster

netcat

- net utility which reads and writes data across network connections
- feature-rich network debugging and exploration tool
- can create almost any kind of connection
- provides access to the following main features:
  - Outbound and inbound connections, TCP or UDP, to or from any ports.
  - Featured tunneling mode which allows also special tunneling such as UDP to TCP, with the possibility of specifying all network parameters (source port/interface, listening port/interface, and the remote host allowed to connect to the tunnel.
  - Built-in port-scanning capabilities, with randomizer.
  - Advanced usage options, such as buffered send-mode (one line every N seconds), and hexdump (to stderr or to a specified file) of transmitted and received data.

Netcat is distributed freely under the GNU General Public License

RMON

- **RMON (Remote MONitoring) SNMP based Standard**
- **Erlaubt Management von Netzwerk Verkehr**
- **Wird in einer MIB gespeichert**
- **SNMP wird benutzt um virtuelles Device zu managen**
- **9 Gruppen von MIBs (SubMibs)**
- **Gerät unterstützt bereits RMON, wenn es eine dieser Gruppen unterstützt**
- **Daher Begriff des „full 9-group RMON“**

RMON Gruppen

- Statistics
  - Basis Ethernet Statistik (bytes/sec, frames/sec, CRC-errors, cable faults)
- History
  - Aufnahme von History-Informationen (history/trending/logging)
  - Entwicklung spezieller Hardware, da teilweise hoher Speicherverbrauch
- Host/HostTopN/Matrix
  - Host: Monitoring, welcher Verkehr von Mac-Adressen produziert wird
  - HostTopN: Summary-Info über den Tag (die n aktivsten Rechner)
  - Matrix: N zu N Mac-Address Info (sehr speicherintensiv)
- Filter/Capture
  - Spezifiziert welche Filter benutzt, bzw. welche Interfaces ge“captured“ werden
- Alarm/Event
  - Info, wann alarmiert, bzw. in welcher Event-Group gespeichert wird

RMONv2

- Erweiterung des Verkehrsmanagement nach RMON Standard auf IP und OSI Anwendungs-Layer
- Erfordert die Fähigkeit Ebene 3 Protokolle verarbeiten und Anwendungsprotokolle verstehen zu können

RMON-Sniffer ?

- Generell kann RMON für sniffing benutzt werden
- Ursprünglich als remote sniffer gedacht
  - Stand-alone box (probe)
- Heute vornehmlich als add-on Produkt zu Hubs, Switches und Routern
- Problem:
  - zu langsam im Sniffern,
  - zu rudimentär
  - zu aufwendig bei der Übertragung zur Management-Station

Zusammenfassung

- Mitschneiden von Netzverkehr sowohl in flachen als auch strukturierten Netzen möglich
- Geeignete Software als Plug And Play Tools frei verfügbar
- Physikalischer Zugriff nicht notwendig, da Tools remote steuer- und abrufbar.
- Nur Netzwerkzugriff auf ein geeignetes Gerät erforderlich

Es war nie so einfach wie heute, Daten aus dem Netz mitzulesen.