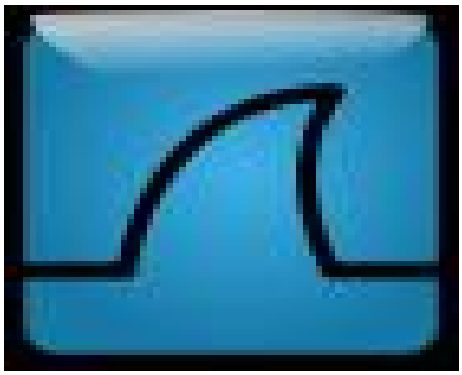
<u>Netzwerksniffer</u>

Einsatz- und Auswertungsmöglichkeiten von Netzwerksniffern

am Beispiel von Wireshark



von Maria-Anna Schano

und

Manuel Heinrich

Inhaltsverzeichnis

1. Definition von Netzwerksniffer....3
2. Einsatzmöglichkeiten von Netzwerksniffern....3
3. Einsatz von Netzwerksniffern....3
4. Netzwerksnifferarten....5
5. Die bekanntesten Netzwerksniffer....5
6. Wie kann ich mich vor Sniffern schützen?....6
7. Erkennen von Snifferangriffen....6
7. Was ist Wireshark....8
7.1 Geschichte von Wireshark....8
7.2 Vorgehensweise von Wireshark....9
7.3 Einführung in Wireshark....10
8. Szenariobeschreibung:....15
8.1 Szenario 1 -via Telnet-:....15
8.1.1 Aufzeichnungsdaten der Telnetverbindung:....16
8.1.2 Filtern der Telnetverbindungsdaten....17
8.1.3 Auswerten der Telnetverbindungsdaten....18
8.2 Szenario 2 -via SSH-:....20
8.2.1 Aufzeichnungsdaten der SSH-Verbindung:....21
8.2.2 Filtern der SSH-Verbindungsdaten....22
8.2.3 Auswerten der SSH-Verbindungsdaten....23
9. Fazit....24
10. Quellenverzeichnis....25
11. Abkürzungsverzeichnis....26
12. Fremdwörtererklärung....27

1. Definition von Netzwerksniffer

Wörtlich aus dem englisichen übersetzt bedeuted „Sniffer“ nichts anderes wie Schnüffler; aber sinngemäß ist in diesem Fall eher abhören gemeint.

Seit Ende der 80er Jahre gibt es Netzwerksniffer (kurz „Sniffer“ genannnt), grundsätzlich geht es bei Netzwerksniffern um Anwendungen, die den Datenverkehr im Netzwerk abhören.

Somit handelt es sich um ein Werkzeug für eine Netzwerkanalyse.

Es gibt diese in Form von Hard- und Software. Heut zu Tage ist die Softwarevariante am meisten verbreitet.

2. Einsatzmöglichkeiten von Netzwerksniffern

Da Netzwerksniffer auf den OSI-Schichten 2 und 3 agieren können diese Netzwerkpaket und -daten empfangen, einlesen und auch aufgezeichnen. Diese Daten können Informationen über die Netwerkkommunikation, Verbindungsarten und -konfiguration enthalten, was eine Fehlersuche im Netzwerk ermöglicht. Aber auch private Informationen wie Benutzernamen und Kennwörter können preisgeben werden; sofern diese nicht verschlüsselt sind.

3. Einsatz von Netzwerksniffern

Am einfachsten lässt sich ein Netzwerk sniffen wenn Hubs als Netzwerkssegmente zwischengeschaltet sind. Bei anderen Netzwerksegmenten wie bei einem Switch bekommt man im Normalfall Probleme den Netzwerkverkehr abzuhören, da der Switch die Daten vom Sender nur an den tatsächlichen Empfänger weiterleitet. Somit würde man nur die eigenen Daten, sowie unwichtigeren Netzwerkverkehr wie z. B. Broadcasts aufzeichnen.

Für diesen Fall haben viele Switchhersteller und Routerhersteller Switchs bzw. Router mit einer Monitorfunktion in Ihrem Portfolio. Damit ist es möglich Netzwerkdaten eines gewünschten Ports auf einen anderen zu spiegeln. Auf diesen gespiegelten Port kann man nun direkt zugreifen.

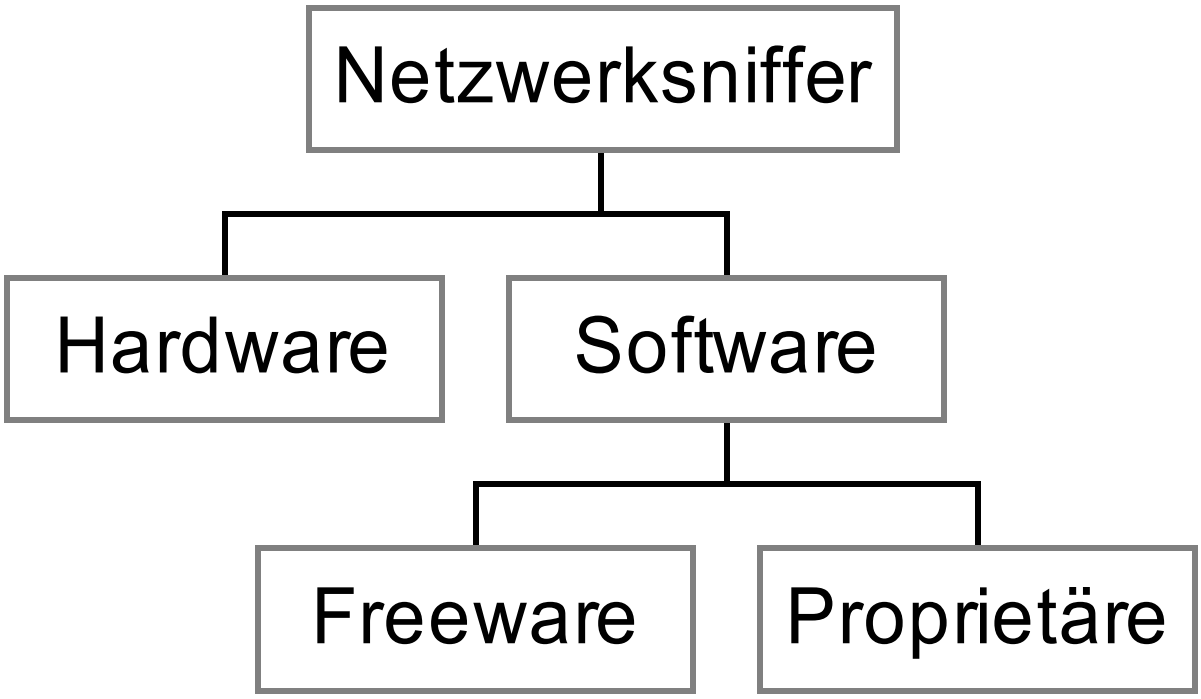
Es gibt aber noch andere Möglichkeiten die oben genannte Problematik zu beseitigen. Möchte man beispielsweise gezielt einen Rechner sniffen, genügt es eine unsichere Verbindung wie über Telnet aufzubauen. Wenn man beabsichtigt das gesamte Netzwerk zu sniffen, muss man auf drastischere Methoden zurück greifen. Davon gibt es heut zu Tage einige, die bekanntesten Methoden sind Spofing-Angriffe wie „ARP-Spoofing“ und „MAC-Flooding“.

Mit einschlägigen Programmen wie Ettercap ist ein ARP-Spoofing möglich. Beim ARP-Spoofing werden mittels manipulierter ARP-Frames der ARP-Cache eines Switches verändert. So kann man dem Switch die IP-Adresse eines Default-Gateways anstelle der eigenen IP-Adresse vorgaukeln. Somit sendet der Switch die Daten nicht direkt an den Empfänger sondern schickt die Daten an den vorgegaukelten Default-Gateway. Der Sniffer erhält wie gewollt die Daten. Um eine abhörbare Verbindung zu schaffen muss aber der Sniffer die Daten an den tatsächlichen Empfänger weiterleiten; sonst sind die Daten verloren und es kann keine Netzkommunikation (die ein Sniffer ja haben möchte) sinnvoll aufgezeichnet werden.
-> Diese Angriffsform gehört zu den “Man-In-The-Middle-Angriffen“.

Beim der Mac flooding werden gefälsche MAC-Daten an den Switch gesendet bis der interne Speicher voll und überfüllt ist. Wenn dies so weit ist, schaltet der Switch in einen „Failopen Mode“. Sobald dies der Fall ist, werden alle Netzwerkdaten, egal ob Unicast oder Broadcast an alle Netzwerkteilnehmer gesendet; so wie bei einem Hub.

Es ist zu beachten; dass das Abhören von Netzwerkverkehrsdaten ohne Einverständis gemäß Telekommunikationsgesetz eine Straftat ist.

4. Netzwerksnifferarten



5. Die bekanntesten Netzwerksniffer

Freeware	***Proprietäre Produkte:***
- Wireshark (früher Ethereal) - Ettercap - NETCORtools (TCP Trace basierend) - Tcpdump	- caplon (consistec) - Clearsight Analyzer (Clearsight Networks) - EtherPeek - OmniPeek - GigaPeek (Wild Packets) - LABdecoder32 (Triticom) - Microsoft Network Monitor - NetSpector (INAT)

6. Wie kann ich mich vor Sniffern schützen?

Leider gibt es vor Sniffer-Angriffen keinen wirklichen Schutz. Allerdings kann man es den Sniffern erschweren indem man verschlüsselte Verbindungen wie SSL (Secure Socket Layer) nutzt oder für Angriffe auf den OSI-Layer 2 sogenannte „Private VLANs“ (PVLAN) nutzt. Dies verhindert zwar nicht das Abören und Aufzeichnen, aber die aufgezeichneten Daten sind ohne Mehraufwand unbrauchbar.

7. Erkennen von Snifferangriffen

Einen sehr guten Snifferanwender kann man so gut wie gar nicht aufspüren. Glücklicherweise sind die meisten von ihnen nicht so gut wie sie selbst vieleicht meinen. Durch Verfahren wie:

- DNS-Lookup
  Hierbei schickt man Daten an einen nicht existierenden Host. Sollte man eine Antwort hierauf erhalten, muss man davon ausgehen, dass eine Station dazwischen geschaltet ist, die auf nicht für sie bestimmte Netzwerkdaten lauscht. Da Netzwerksniffer die IP-Adressen versuchen gleich zu einem Hostnamen aufzulösen .
- Promiscuous-Mode
  Dabei handelt es sich um einen Empfangsmodus einer Netzwerkkarte. Im diesem Modus werden alle Daten an das Betriebssystem übergeben.
  *Im Normalfall werden alle ARP-Daten an die Ethernet-Broadcast-Adresse (FF:FF:FF:FF:FF:FF) geschickt und bearbeitet. Schickt man die ARP-Daten an eine falsche Ethernet-Broadcast-Adresse (z. B. FF:FF:FF:FF:FF:F**A**), sollte die Netzwerkkarte im normalen Modus diese Pakete ignorieren, sollte man eine Antwort erhalten ist die Netzwertkkarte im Promiscuous-Mode und ein Indiz dafür, dass Sie Opfer eines Angriffes wie z. B. eines Sniffer sind.*

- Honeypots (Köderlegung)

  Bei Honeypots (auch Iron Box) zu deutsch auch Honigtopf genannt handelt es sich um ein Programm, wie z. B. mwcollect, das Netzwerkdienste und auch Rechnernetze simuliert. Hat man den Verdacht, dass man Opfer eines Sniffers ist setzt man ein solches Programm zur „Köderlegung“ ein, da Zugriffe auf die simulierten Dienste z. B. falsche IP-Adressen und die damit verbundenen Aktionen protokolliert und gegebenefalls einen vordefinierten Alarm auslöst.

ist es möglich einen Sniffer(angrif) zu erkennen.

7. Was ist Wireshark

Wireshark wörtlich aus dem Englischen übersetzt bedeuted „Kabelhai“ und ist ein kostenloses Programm zur Analyse von Netzwerkkommunikationsverbindungsdaten. Daher zählt es zur Programmgruppe der Netzwerksniffer.

Dies ist das Logo von Wireshark:

Es kann kostenlos unter: „http://www.wireshark.org/download.html“ heruntergeladen werden.

7.1 Geschichte von Wireshark

Ursprünglich war Wireshark unten den Namen „Ethereal“ bekannt. Ethereal wurde von der Firma Ethereal Software unter der Leitung von Gerald Combs als GNU-Lizenz (General Public License) entwickelt. Als Gerald Combs im Jahre 2006 von Ethereal Software Inc. zu CACE Technologies wechselte, startete er gleich ein eigenes Folgeprojekt und nannte es Wireshark.

Wireshark verdrängte viele Netzwerkanalyseprogramme kommerzieler Hersteller vom Markt, da dieses Open-Source-Produkt von Bedienung, Erscheinungsbild und Wirkungsweise jedem dieser Programme ebenbürdig war und zumal war es kostenlos.

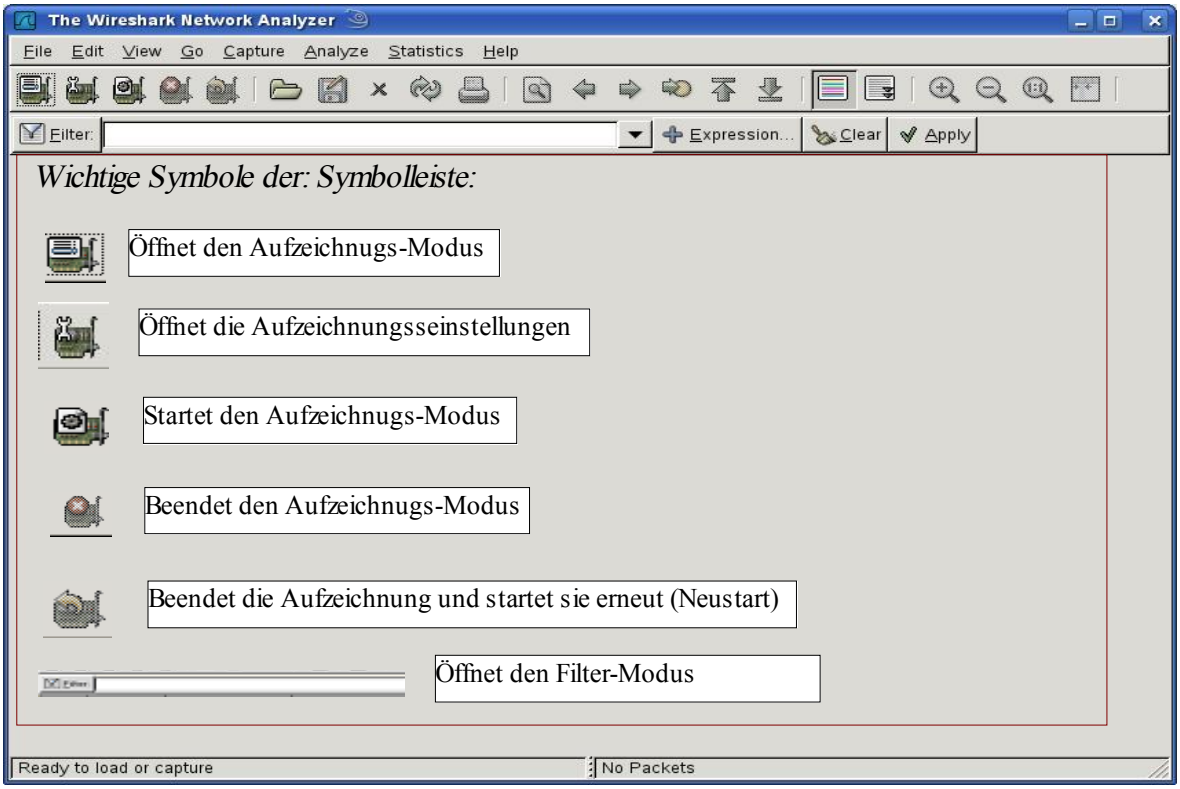
Heute (Januar 2009) ist Wireshark noch immer kostenlos und in der Version 1.0.4 für die drei gängigsten Betriebssysteme Linux, Mac OS und Windows erhältlich. Für Windows wird sogar eine portable Version angeboten, die nicht einmal installiert werden muss. Die Version 1.1.1. ist derzeit im Entwicklungsstatus und soll im Frühjahr 2009 erscheinen.

7.2 Vorgehensweise von Wireshark

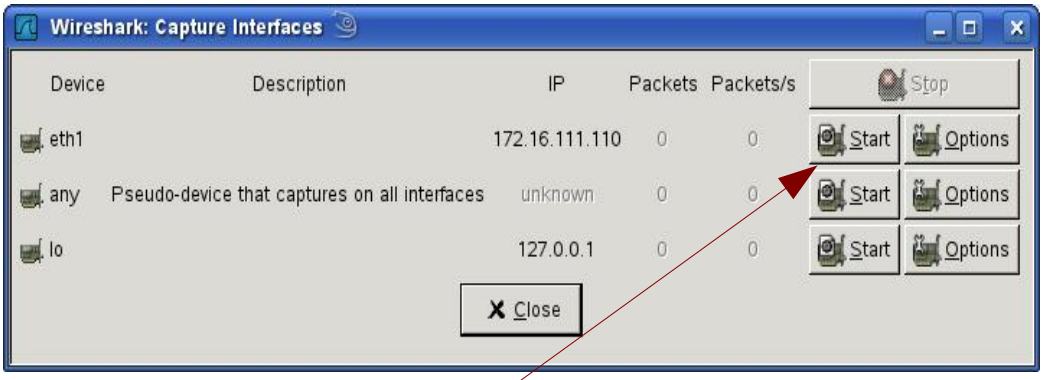
Wireshark stellt nach der Aufzeichnung des Datenverkehrs einer Netzwerk-Schnittstelle (meist eine Ethernet-Netzwerkkarte mit TCP/IP) die Daten in Form einzelner Pakete dar. Dabei werden die Daten übersichtlich und für den Menschen nachvollziehbar zum Analysieren dargestellt. D. h. so kann der Inhalt der mitgeschnittenen Pakete betrachtet oder nach Inhalten gefiltert werden.

7.3 Einführung in Wireshark

Startbildschirm von Wireshark

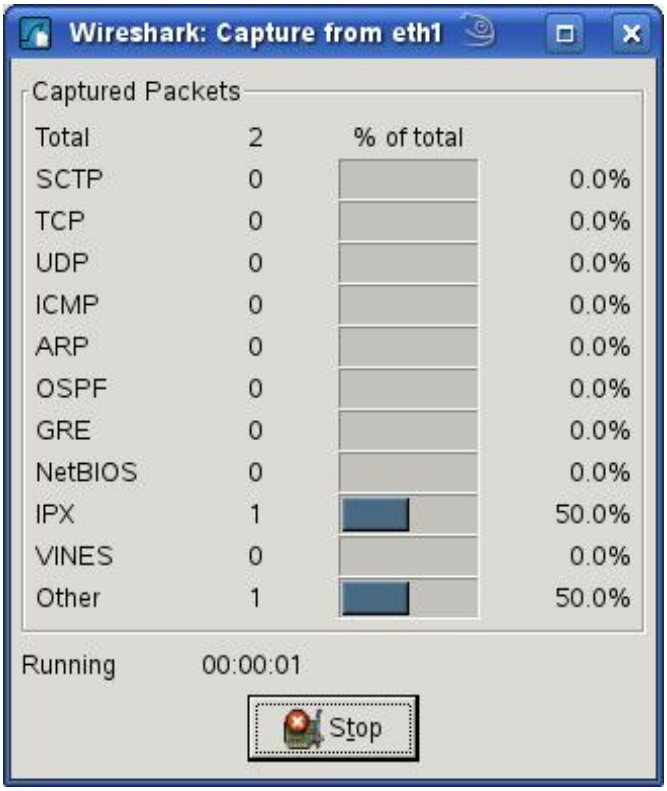


Bildschirm des geöffneten Aufzeichnungs-Modus



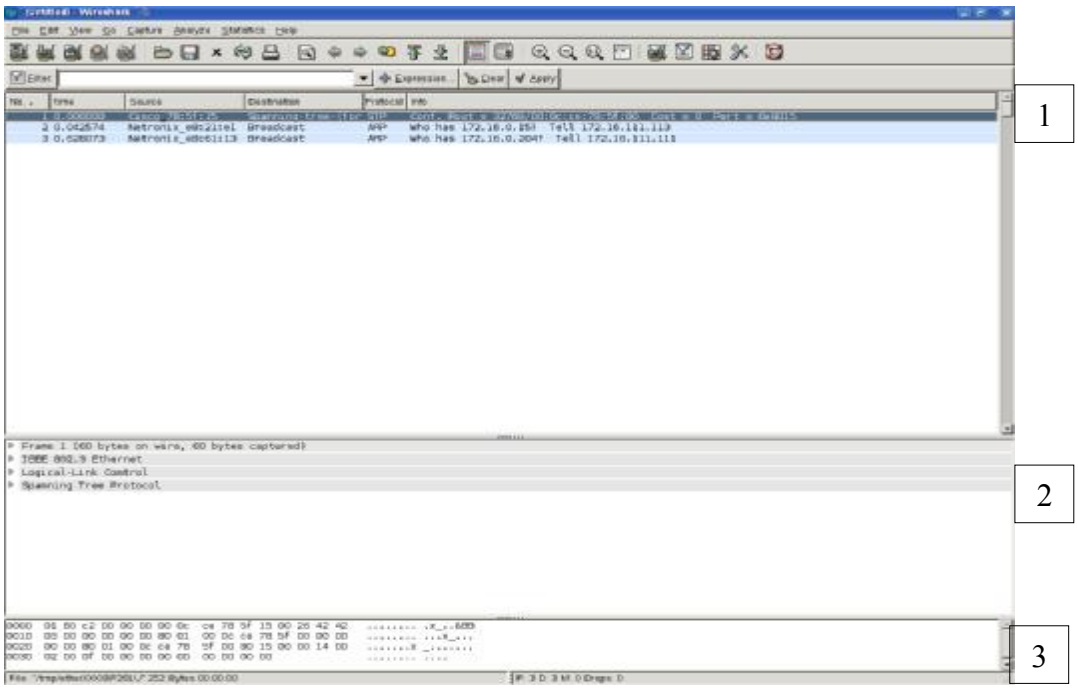
Durch drücken des -Buttons wird der Aufzeichnungs-Modus geöffnet

Bildschirm des gestarteten Aufzeichnungsmodus



Hier sieht man welche und wieviele Protokollpakete derzeit aufgezeichnet sind

Daten des Aufzeichnungs-Modus (Beispiel)



Der Bildschirm, in dem die aufgezeichneten Daten bearbeitet und analysiert werden, wird ist in 3 Bereiche aufgeteilt.

1 Paketliste

In der Paketliste, sieht man alle aufgezeichneten Frames. Die Spalten geben folgende Informationen preis:

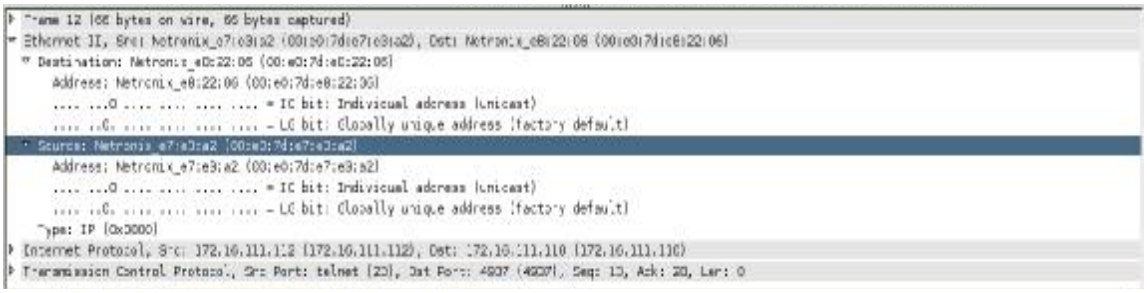
1. No. = ist eine fortlaufende Nummerierung der Frames
2. Time = zeigt den Zeitabschnitt der Aufzeichnung an
3. Source = zeigt den Absender eines Frames an (meist die IP)
4. Destination = zeigt den Empfänger des Frames an (meist die IP)
5. Protocol = zeigt das verwendete Protokoll des Frame an
6. Info = gibt zusätzliche Informationen zum Frame bekannt.

–

1 2 3 4 5 6

2 Paketdetails

In den Paketdetails werden die Layer (Schichten) des Datenframes angezeigt. Durch anklicken des Pfeil-Symbols kann der gewählte Layer erweitert werden.



Die Protokolledetails varieren von Protokoll zu Protokoll. Denoch sind die ersten zwei Layer:

- Frame

  Hier sind Informationen von Wirehsark zum betreffenen Frame. Unter andrem erkennt man hier die Größe des Frames, Zeit und die Zeitdifferenz zum vorrangegangen Frame.

- Ethernet II

  Zeigt Infomrationen zum OSI-Layer 2 (Sicherungsschicht). Im wesentlichen sieht man hier die MAC-Adressen des Absenders und des Empfängers; aber im Normallfall wird die MAC-Adresse des Empfängers die des Default Routers sein..

immer gleich.

Wie bereits oben erwähnt varieren die übrigen Paketdetails von Protokoll zu Protokoll, daher werden wir das TCP-Protokoll als Beispiel näher erläutern.

Beim TCP-Protokoll finden wir vier Paketdetails wieder (siehe oben gezeigt Abbildung). Auf die ersten beiden Layer die stets gleich sind sind wir schon näher eingegangen. Bei den anderen beiden Layer handelt es sich um:

- Internet Protokoll (IP)

  Dieses Layer gibt Außschluss zum OSI-Layer 3 und gibt Angaben wie die IP-Adresse des Absenders und Empfängers sowie die Lebenszeit (TTL) preis.

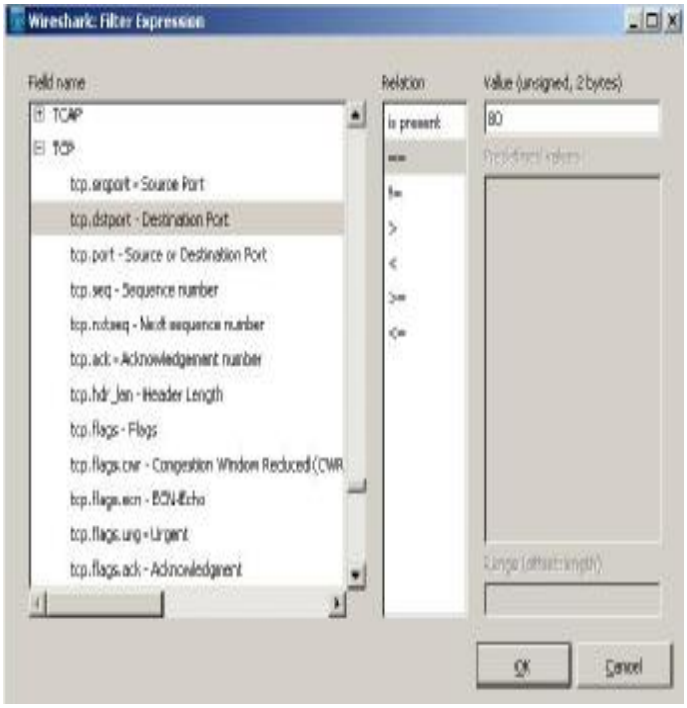
- Transmission Controll Protokoll (TCP)

  Das Layer zeigt Informationen sogar zum OSI-Layer 4 und zeigt alle Informationen zur ENDE-ZU-ENDE Verbindung an. Darüber hinaus werden die Ports preisgegeben.

3 Erläuterung zu dem Hexadezimale Paketanzeige

Hier sind die Daten einmal im Hexadezimalsystem (links) und nebendran im Klartext (rechts) bzw. in entschlüsselter Form angezeigt.

Die Filter:



Durch einen Klick auf das Filtersymbol öffnet sich ein Fenster in dem eine Vielzahl an Filterungsmöglichkeiten möglich sind.

z. B. Kann man gezielt nach gewissen IP´s oder Protokollen suchen.

8. Szenariobeschreibung:

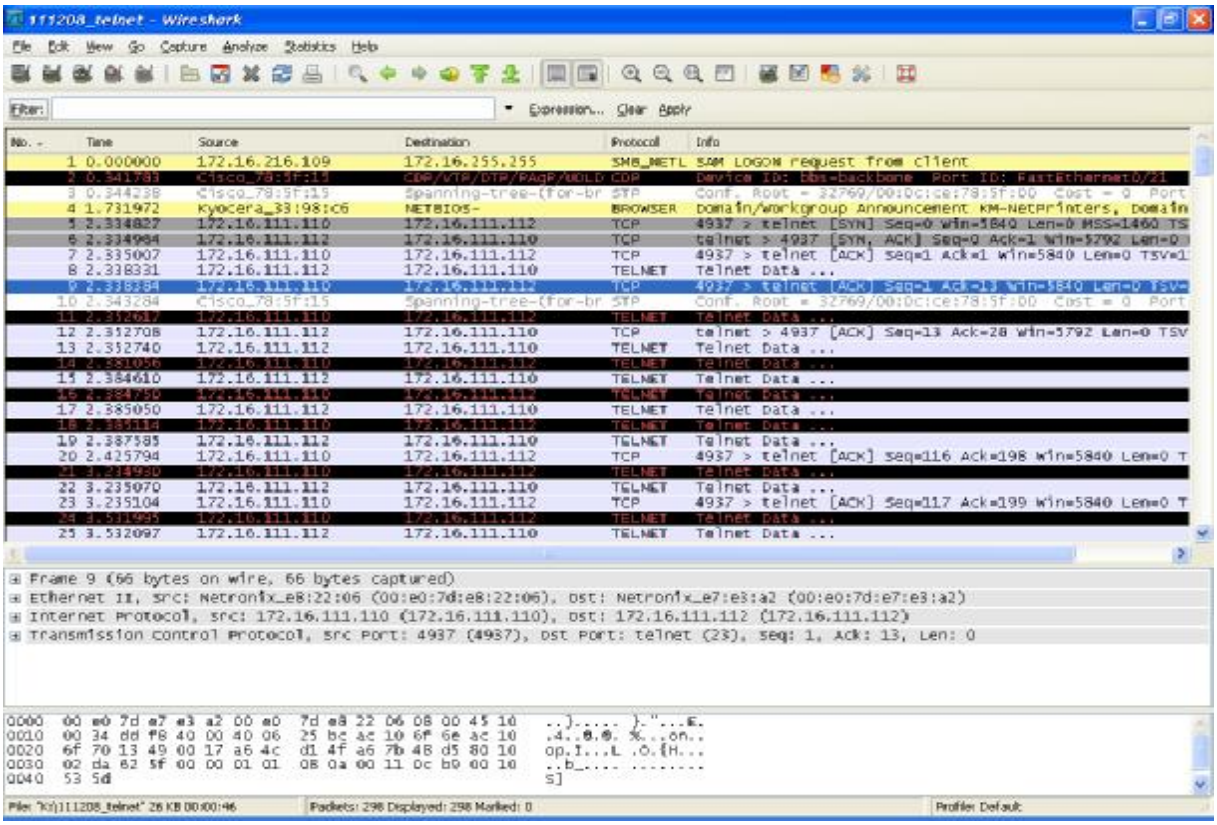
In unserem Szenario werden wir unter der Linuxdistribution „Open Suse 10“ unter zur Hilfenahme von Wireshark, eine Verbindung von Rechner „A“ (IP: 172.16.111.110) zu Rechner „B“ (IP: 172.16.111.112) aufzeichnen und auch auswerten. Zum besseren Verständnis werden wir hierzu eine Verbindung via Telnet und einmal via einer SSH-Verbindung vergleichen.

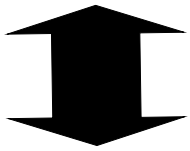
8.1 Szenario 1 -via Telnet-:

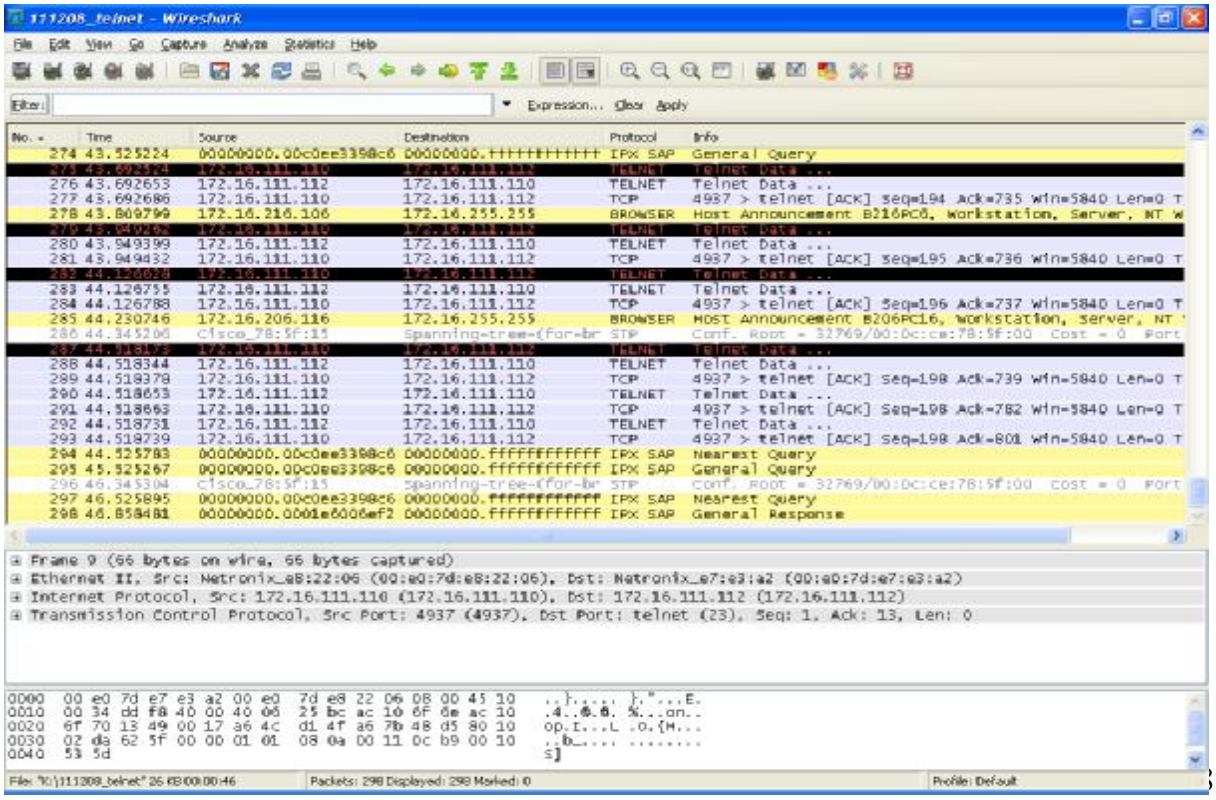
Zum Start dieses Szenario wurde bereits auf Rechner „B“ ein Telnetserver gestartet. Nachdem Wireshark von Rechner „A“ gestartet wurde loggen wir uns mit dem Benutznamen „bbs“ mit dem dazugehörigen Passwort „Brille“ von Rechner „A“ auf Rechner „B“ via einer Telnetverbindung ein. Anschließend werden wir diese Verbindung auswerten.

Hinweis: Telnet (Telecommunication Network) ermöglichst eine Verbindung zwischen zwei Rechnern über ein Netzwerk.

8.1.1 Aufzeichnungsdaten der Telnetverbindung:

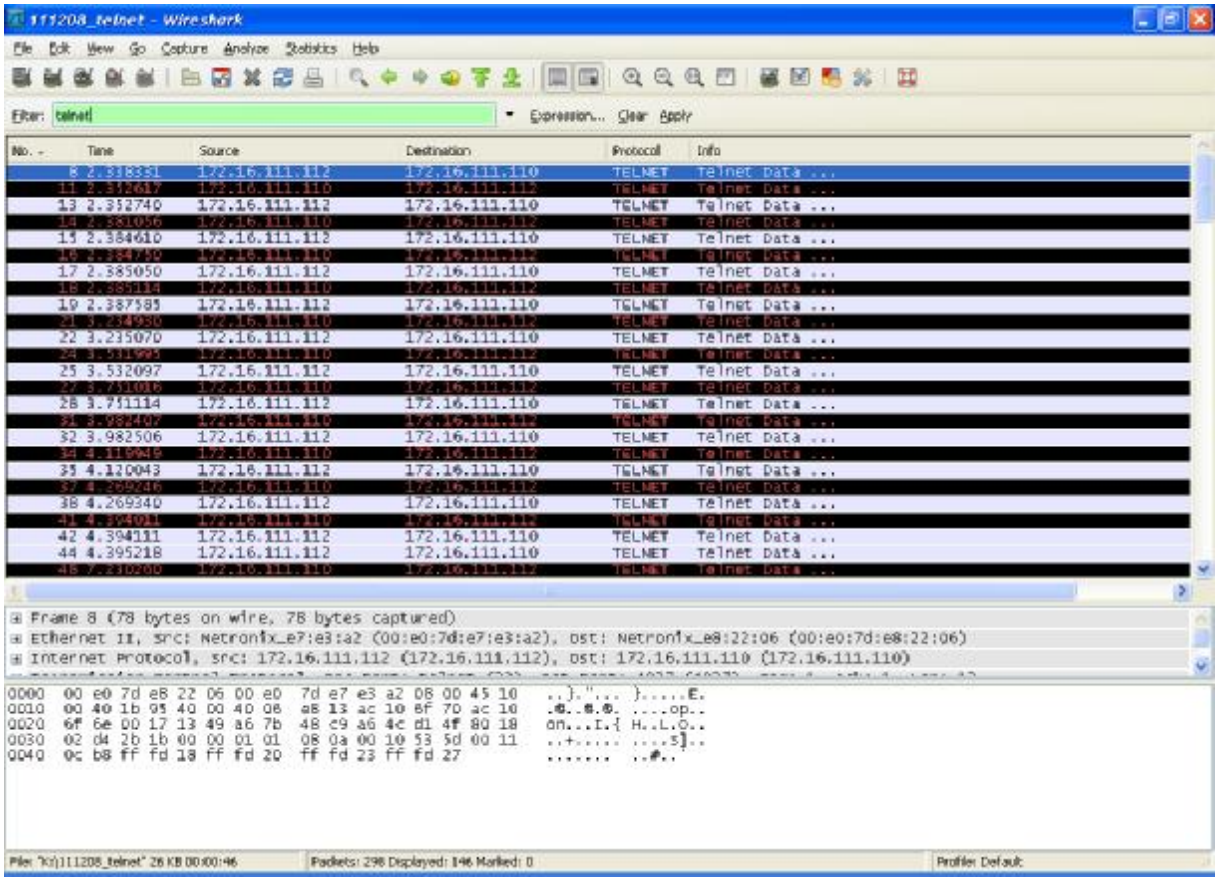






8.1.2 Filtern der Telnetverbindungsdaten

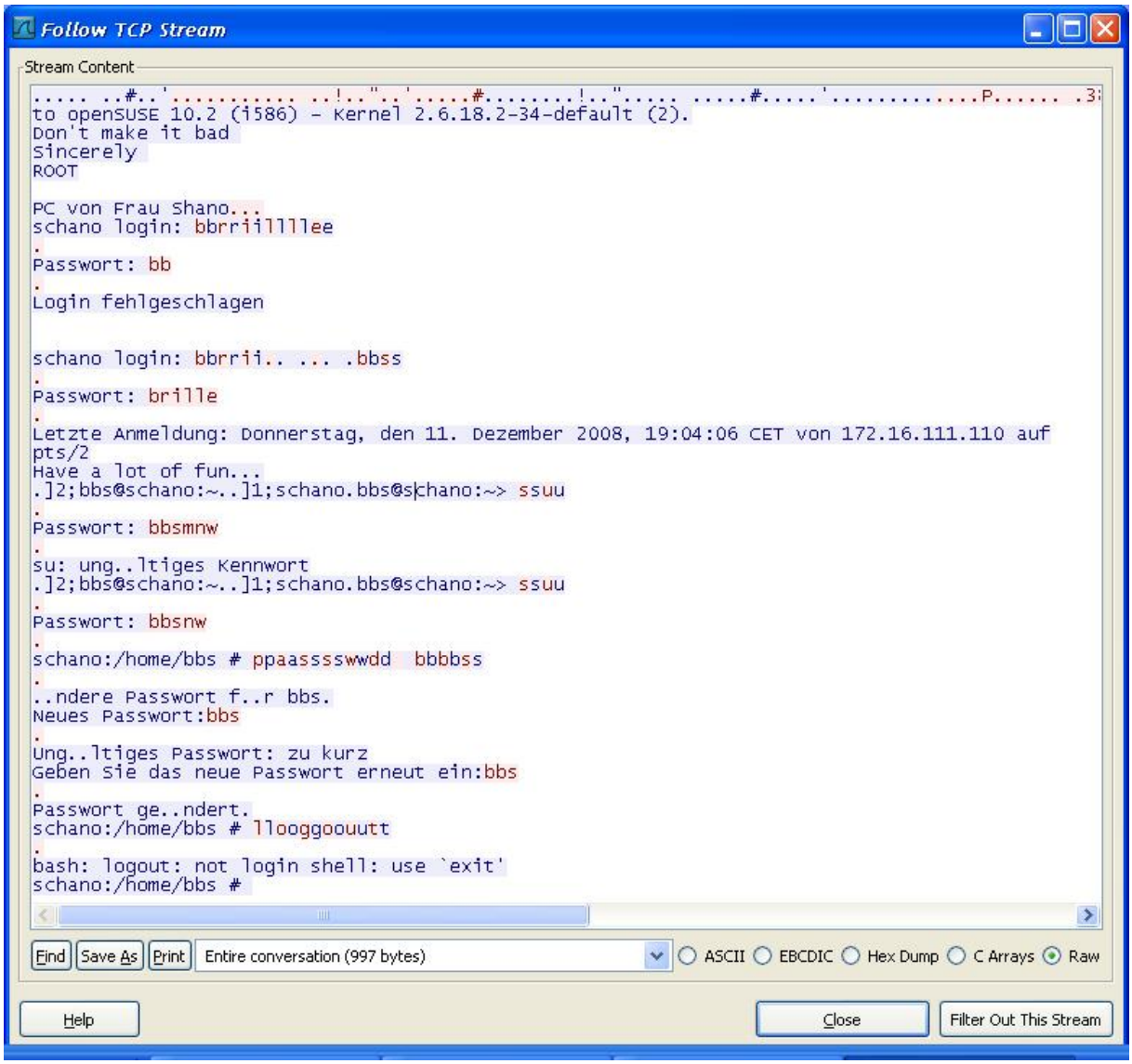
Da die Aufzeichnungsdaten sehr umfangreich sind, setzen wir bewusst einen Filter. In diesem Falle, verwenden wir einen Protokollfilter und filtern gezielt nach dem Telnetprotokoll.



8.1.3 Auswerten der Telnetverbindungsdaten

Nachdem wir den Filter gesetzt haben, können wir jetzt im Kontextmenü die Funktion „Follow TCP Stream“ wählen.

Nun öffnet sich ein neues Fenster, in dem man die Aufzeichnung im Klartext angezeigt bekommt. An dieser Stelle sind die beiden unterschiedlichen Schriftfarben zu beachten. In den Standartfarbeinstellungen, welche wir verwenden, symbolisiert ist die blaue Schriftfarbe die Framedaten des Empfängers und die rote Schriftfarbe die Framedaten des Senders.



Nun können wir den aufgezeichneten Telnet-Verbindungsaufbau auswerten.

Wie wir erkennen können, wurde sich zuerst mit dem falschen Namen und dem falschen Passwort angemeldet. Wie zu erwarten war ist der Loginversuch fehlgeschlagen. Beim zweiten Versuch wurde sich ordnungsgemäß mit Benutzname „bbs“ mit dem dazugehörigen Passwort „Brille“ angemeldet.

-> Das richtige Passwort „Brille“ wurde ebenso wie das zuvor falsche Passwort im Klartext übertragen.

Anschließend haben wir vom Benutzer „bbs“ auf den Benutzer „root“ gewechselt und haben das Passwort für den Benutzer „bbs“ von „Brille“ auf „bbs“ gewechselt. Zum Schluss haben wir uns wieder abgemeldet.

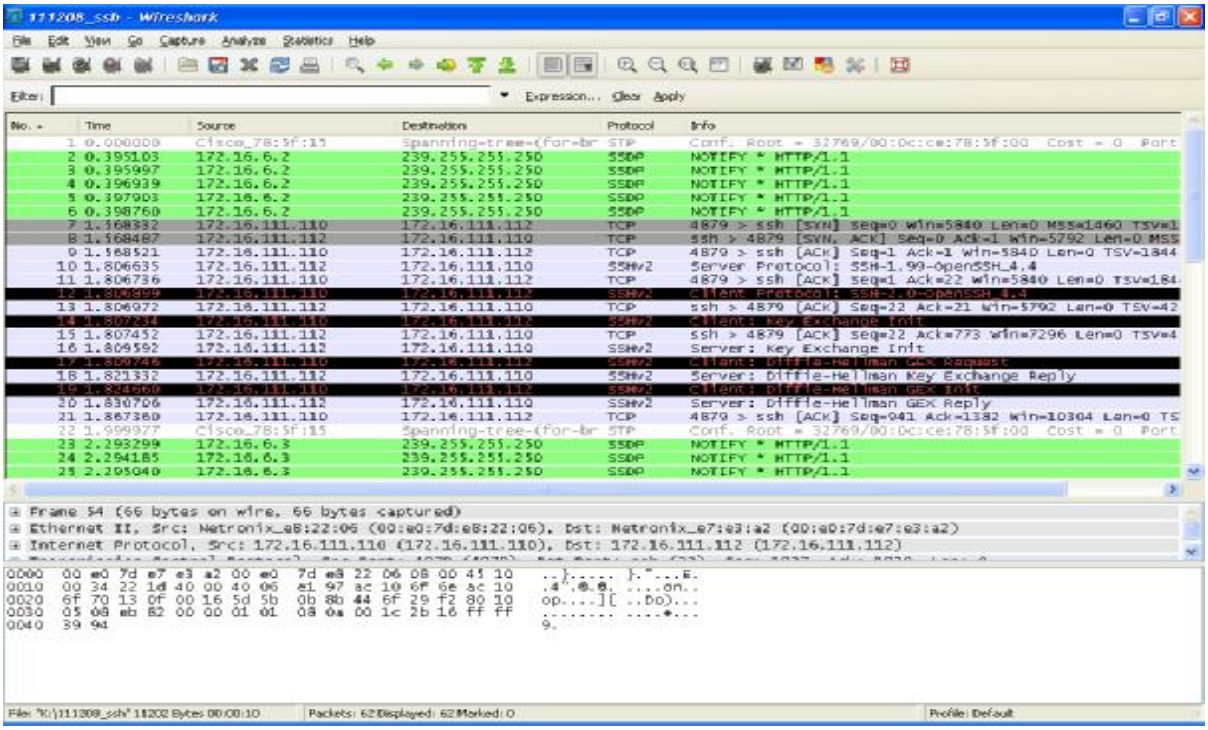
-> Bis auf Darstellngsfehlern bei den Umlauten (ä, ö, ü) wurde die gesamte Telnetverbindung im Klartext aufgezeichnet.

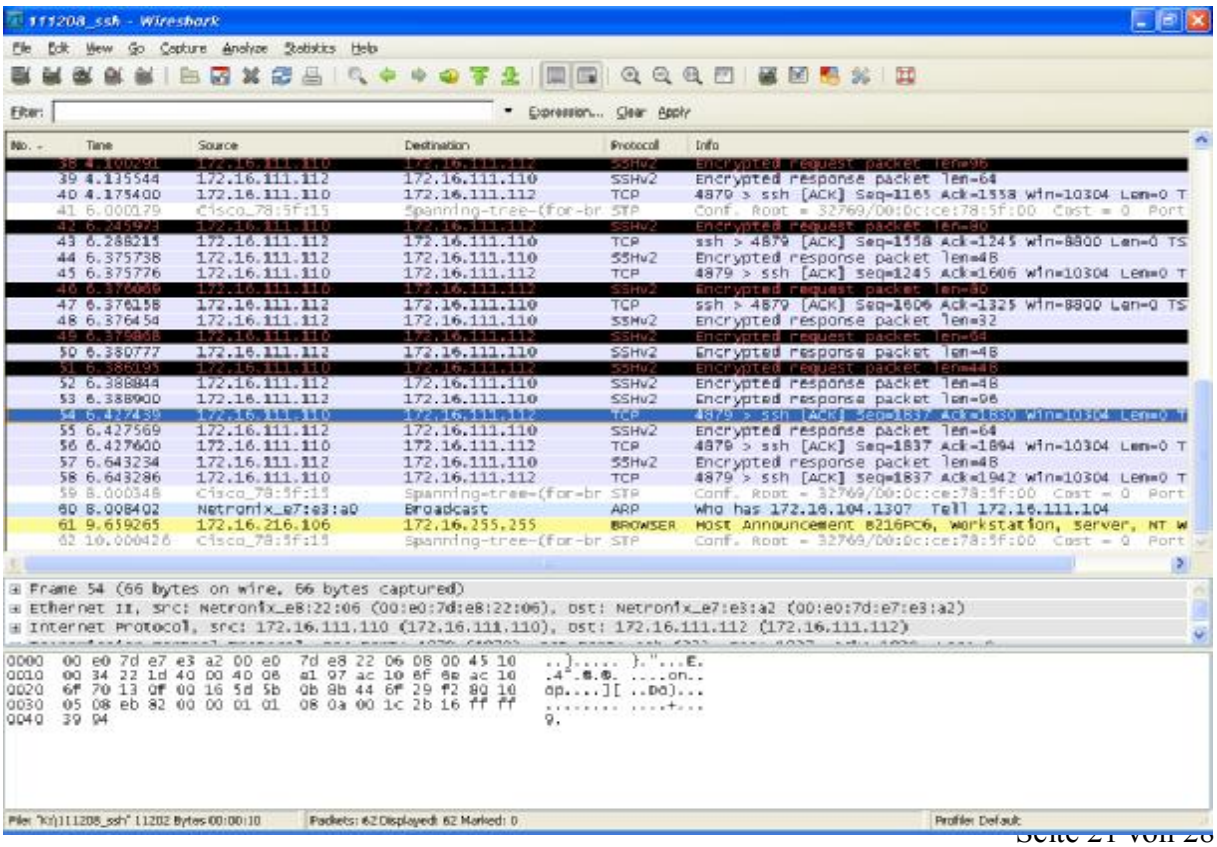
8.2 Szenario 2 -via SSH-:

Zum Start dieses Szenario wurde bereits auf Rechner „B“ ein SSH-Server gestartet. Nachdem Wireshark von Rechner „A“ gestartet wurde loggen wir uns mit dem Benutznamen „bbs“ mit dem dazugehörigen Passwort „Brille“ von Rechner „A“ auf Rechner „B“ via einer SSH-Verbindung ein. Anschließend werden wir diese Verbindung auswerten.

Hinweis: SSH (Secure Shell) ermöglicht eine sichere, authentifizierte und verschlüsselte Verbindung zwischen zwei Rechnern über ein Netzwerk

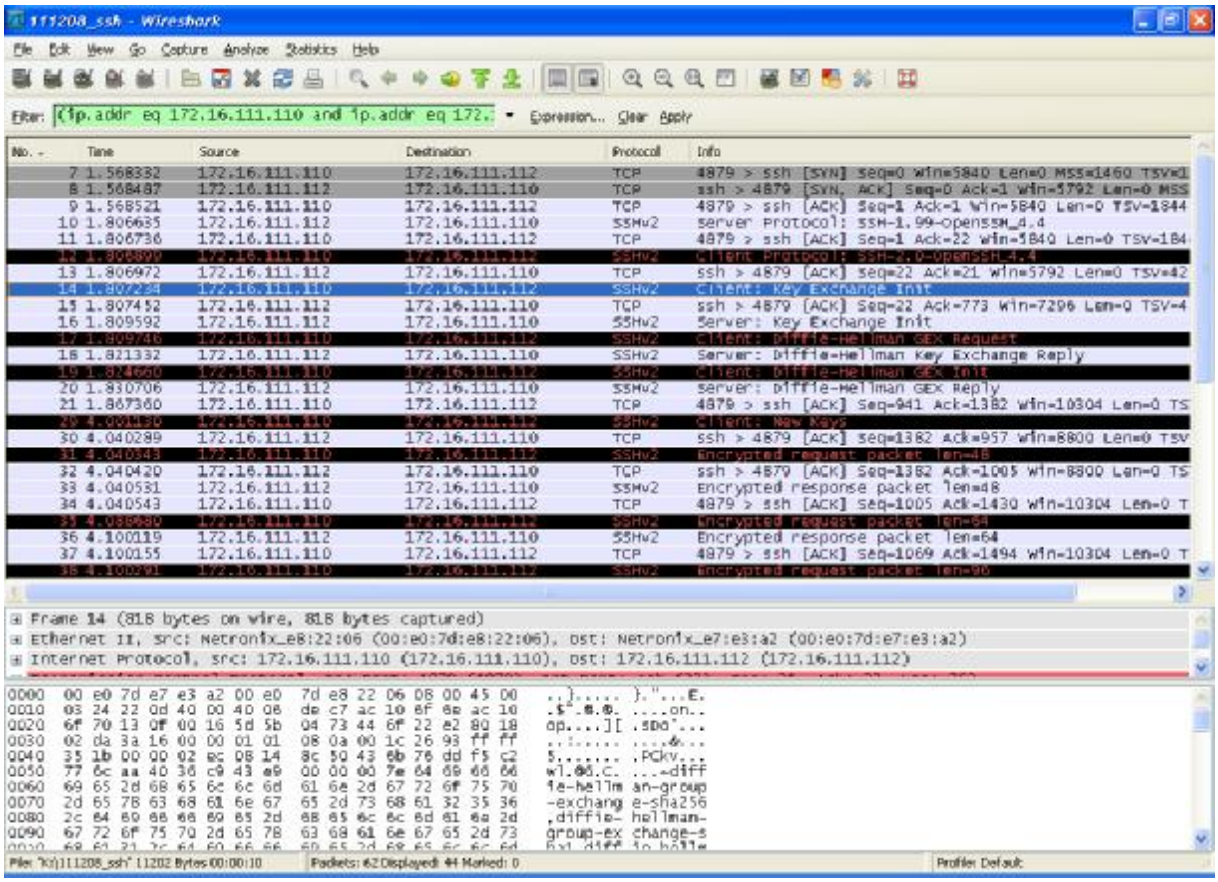
8.2.1 Aufzeichnungsdaten der SSH-Verbindung:





8.2.2 Filtern der SSH-Verbindungsdaten

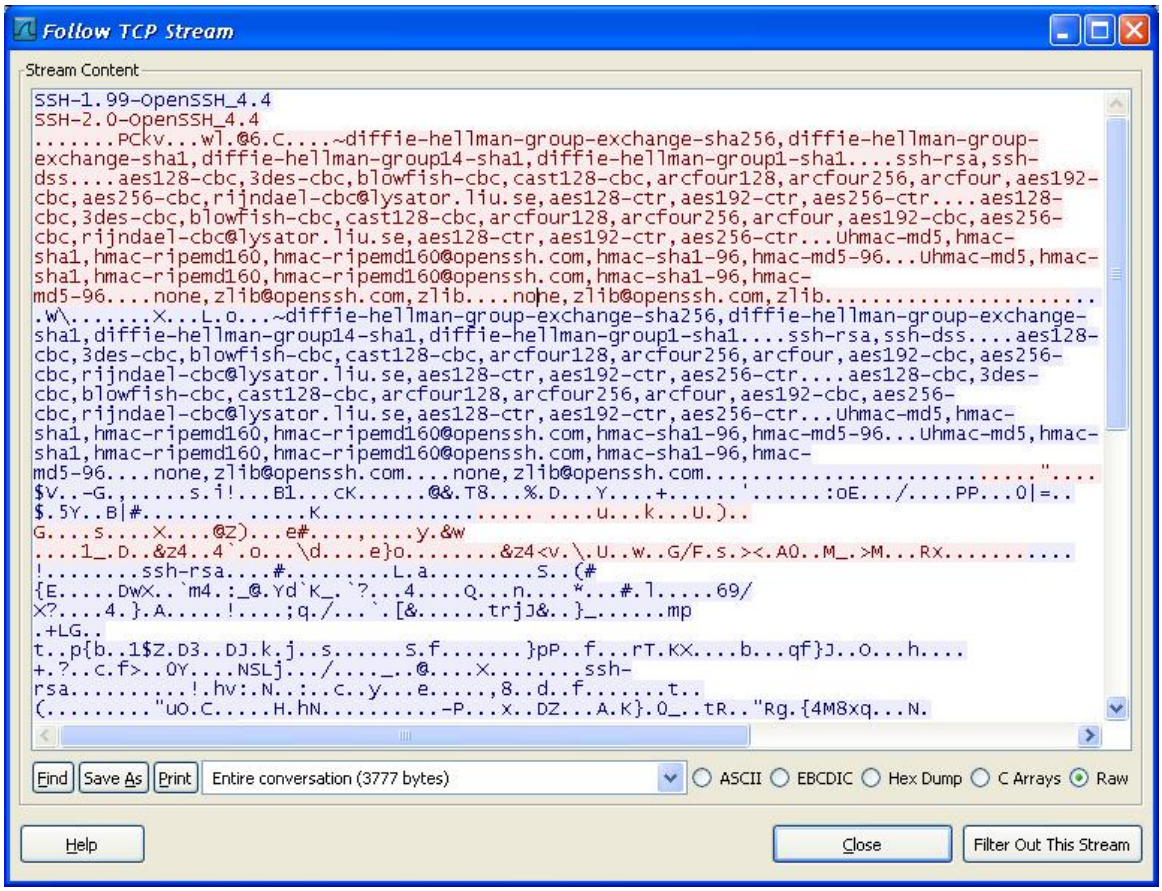
Da die Aufzeichnungsdaten auch hier sehr umfangreich sind, setzen wir auch hier bewusst einen Filter. In diesem Falle, verwenden wir einen Protokollfilter und filtern gezielt nach SSH-Protokollen.



8.2.3 Auswerten der SSH-Verbindungsdaten

Nun öffnen wir auch hier im Kontextmenü die Funktion „Follow TCP Stream“..

Wie bei der Telnetverbindung auch öffnet sich jetzt ein neues Fenster mit den SSH-Verbindungsdaten.



Da die Aufzeichnung nur verschlüsselt aufgezeichnet wurde, ist eine Auswertung nicht ohne weiteres möglich. Man benötigt an dieser Stelle einen Cracker oder sonstige Hacker-Software, auf die wir hier nicht weiter eingehen und beenden somit unsere „Szenario 2“.

9. Fazit

Generell kann man sagen, dass Netzwerksniffer das halten, was Sie versprechen.

Mit dem verwendeten Netzwerksniffer „Wireshark“ hatten wir zu Beginn das Problem, dass dieser unübersichtlich und komplex wirkte. Aber nach einer kurzen Einarbeitunsphase und Recherchen im Internet sind wir mit Wireshark recht gut zurecht gekommen.

Obwohl Wireshark an sich ab und an auf Grenzen stösst ist es möglich diese mit weiteren Programmen zu überwinden.

Z. B. zeichnet Wireshark von Haus aus keine Daten die über einen Switch gehen auf, aber mit anderen Programmen wie beispielsweise dem Programm „Ettercap“ lässt sich dies umgehen. Hierzu macht „Ettercap“ einen „ARP-Spoofing“,

In unseren Szenarios war es uns möglich die Netzwerkdaten aufzuzeichnen. Allerdings war eine Auswertung der aufgezeichneten Daten nur mit den veralteten Protokoll „Telnet“ möglich, da die Daten im Klartext aufgezeichnet wurden. Mit dem neueren Protokoll „SSH“, war es uns ohne erheblichen Mehraufwand nicht möglich die Daten auszuwerten, da die Daten nur verschlüsselt aufgezeichnet wurden.

Daher empfehlen wir, bei Remoteverbindungen auf das SSH-Protokoll zurück zugreifen und auf veraltete Remotverbindungsprotokolle wie „Telnet“ zu verzichten, da dieses u. a. keine Verschlüsselung vornimmt, auch bei Passwörtern. Da dieses Prinzip im Wesentlichen auch für das Surfen im Internet gilt empfehlen wir für sensible Daten sichere Verbindungen wie https zu nutzen.

10. Quellenverzeichnis

Homepage	Datum, Uhrzeit
http://de.wikipedia.org/wiki/Fazit	17.01.2008, 14:53 Uhr
http://de.wikipedia.org/wiki/Honeypot	08.01.2009, 19:34 Uhr
http://de.wikipedia.org/wiki/Promiscuous_Mode	08.01.2009, 19:36 Uhr
http://de.wikipedia.org/wiki/Sniffer	13.11.2008, 19:20 Uhr
http://de.wikipedia.org/wiki/Wireshark	13.11.2008, 19:17 Uhr
http://images.google.de/imgres?imgurl=http://www.vereintestimmen.at/images/schnueffeln.gif&imgrefurl=http://www.vereintestimmen.at/stimmundgesangangebote/einsteiger/index.html&usg=__B4g2fog1B3yqsEmnQ2n_FxDylTs=&h=100&w=122&sz=5&hl=de&start=16&um=1&tbnid=ns9AfmeXx5N_tM:&tbnh=73&tbnw=89&prev=/images%3Fq%3Dschn%25C3%25BCffeln%26um%3D1%26hl%3Dde	15.01.2009, 20:27 Uhr
http://nwlab.net/guide2na/netwerkanalyse-sniffern.html	06.01.2009, 19:42 Uhr
http://www.nwlab.net/tutorials/wireshark/wireshark-tutorial-2.html	15.11.2008, 20:13 Uhr
http://www.tecchannel.de/netzwerk/lan/401719/fehler_im_lan_finden_mit_netzwerk_sniffer/index13.html	08.01.2009, 18:34 Uhr
http://www.tecchannel.de/netzwerk/lan/401719/fehler_im_lan_finden_mit_netzwerk_sniffer/index13.html	08.01.2009, 19:19 Uhr
http://www.wireshark.org/	13.11.2008, 18:45 Uhr

11. Abkürzungsverzeichnis

Abkürzung	**Ausgeschrieben**
ARP	Address Resolution Protocol
DNS	Domain Name System
GNU	General Public License
IP	Internet Protokoll
MAC	Media Access Control
OSI	Open System Interconnection
PVLAN	Private Virtual Local Area Network
SSH	Secure Shell
TCP	Transmission Contol Protocol
Telnet	Telecommunication Network
TTL	Time to Life
u. a.	unter anderem
z. B.	zum Beispiel

12. Fremdwörtererklärung

Fachwort	Erklärung
ausloggen	abmelden
Broadcast	Rundruf an alle Netzwerkteilnehmer
DNS	Internetdienst, bei Anfragen eines Hostnamens gibt der die dazugehörige IP-Adresse weiter
einloggen	anmelden
Flooding	Überflutung
Frame	Datenübertragungsblock
Freeware	kostenlose Software
Gateway	Protollumsetzer, erlaubt Computern und Netzwerken, die auf verschiedenen Protokollen arbeiten miteinander zu kommunizieren
Hub	Ein Multiport-Repeater, der es ermöglicht mehrere Computer mit einander zu Verbinden
Linux	Betriebssystem
Linux-Distribution	Zusammenstellungen von freier Software mit dem Linuxkern
MAC-Adresse	Eingebrannte Adresse auf der Netzwerkkarte, die den Hersteller sowie eine einmalige Netzwerkadresse angibt
Man-In-The-Middle-Angriff	auch **Janusangriff** genannt. Ist eine Angriffsform für Rechnernetzen. Der Angreifer steht dabei physikalisch oder logisch zwischen den kommunizierenden Computern. Er hat dabei mit seinem System die komplette Kontrolle über den Datenverkehr zwischen den

	kommunizierenden Netzwerkteilnehmern.
Portable	Mitnehmbar.
Portfolio	Sortiment
Proprietäre	Lat.proprietarius, franz.proprietaire Eigentümer, jegliche Software, die keine freie Software ist
Remoteverbindung	Fernzugriff
Repeater	Verstärker eines Netzwerksignals
Router	Kann Rechnernetze koppeln und trennen, kann Daten weiterleiten oder blockieren
Spoofing	Manipulation, Verschleierung
Switch	Ein Multiport-Repeater, der es ermöglicht mehrere Computer mit einander zu Verbinden
Unicast	Direkte Verbindung zwischen zwei Netzwerkteilnehmern, Punkt-zu-Punkt-Verbindung