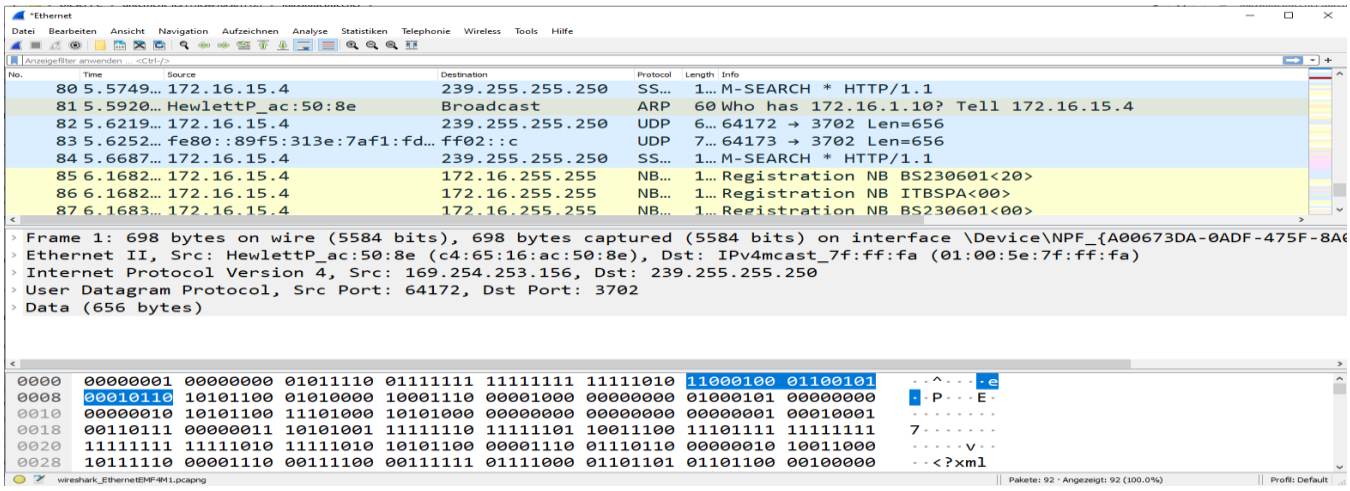
Netzwerkanalyse mit Wireshark – Teil II – TCP/UDP



Mit dem Network-Analyser Wireshark können Sie viele Netzwerk-Abläufe sichtbar machen. In der folgenden Aufgabe sollen Sie die Transportschichtprotokolle TCP und UDP vergleichen.

1. Starten Sie Wireshark auf ihrem PC und starten Sie den Mitschnitt. Nach dem Start führen Sie folgende Aufgaben durch:
   a. Führen Sie innerhalb der CLI den Befehl „nslookup www.iana.org“ aus.
   b. Öffnen Sie einen Browser und gehen sie auf die Seite http://www.passau.de
      Wichtig: öffnen Sie die unverschlüsselte Webseite durch Eingabe von http://...
   c. Führen Sie einen Dateizugriff auf ihr Homelaufwerk am Fileserver durch. Öffnen Sie dazu mit „Windowstaste + r“ den „ausführen“-Dialog. Geben Sie hier den sog. UNC-Pfad zu ihrem Home-Laufwerk ein: „\\itsw16fs01\benutzername$“ wobei Benutzername durch ihre Kennung 21it… ersetzt werden muss.

2. Suchen Sie die Datenpakete, die UDP verwenden.
   a. Welches Anwendungsschichtprotokolle nutzen UDP?

      DNS, LLMNR,

   b. Folgen Sie einem UDP-Stream (rechte Maustaste auf ein UDP-Paket)
      Wie viele Datenpakete gehören zum UDP-Stream?

      2

   c. Welche Pakete sind in einem DNS-Vorgang enthalten?

      Query und Response Pakete

3. Suchen Sie den http-Aufruf auf www.passau.de und folgen Sie dem TCP-Stream.
   a. Wie lautet die Bezeichnung (eckige Klammern) der ersten drei Pakete?

      ACK Acknowledge | SYN Syncronise

   b. Klappen Sie im Protokoll TCP den Bereich Flags aus. Welche Flags sind bei den ersten drei Paketen gesetzt:

      Paket 1: SYN Paket 2: ACK, SYN Paket 3: ACK

c. Welche Ports (Quell- und Zielport) werden verwendet?

Paket 1: Quellport 60230 Zielport: 80

Paket 2: Quellport 80 Zielport: 60230

Paket 3: Quellport 60230 Zielport: 80

d. Bestimmen Sie von den ersten drei Paketen die Sequenz- und Acknowledgement-Nummern.

Paket 1:

e. Sequenz-Nr: 0 Ack-Nr: _____

Paket 2:
Sequenz-Nr: 0 Ack-Nr: 1

Paket 3:
Sequenz-Nr: 1 Ack-Nr: 1

f. In welchem Zusammenhang stehen Sequenznummer und ACK?

Sequenz-Nr ist die Ack-Nr des Vorhergehenden Paketes

g. Bestimmen Sie vom 4. Paket die Sequenznummer und die Länge (Length) der Daten

4. Paket: Sequenz-Nr. 1 Length: 449

h. Ermitteln Sie vom 5. Paket die ACK – Nummer

ACK: 450

i. In welchen Zusammenhang stehen Sequenznummer 4. Paket und ACK vom 5. Paket?

Ack-Nr ist der Payload des Vorgergehenden Paketes + 1

4. Analysieren Sie den Dateizugriff auf den Fileserver. Folgen Sie dazu dem TCP-Stream eines SMB-Protokolls und beantworten Sie folgende Fragen:
   a. Nennen Sie die verwendeten Protokolle auf folgenden OSI-Layern:

      Network-Layer: IPv4

      Transport-Layer: TCP

      Session-Layer: NetBIOS

      Application Layer: SMB2

   b. Welche Ports werden für den SMB-Zugriff verwendet:

      Source-Port: 60379 Dest-Port: 445

   c. Welchem Protokoll bzw. welcher Anwendung wird der sog. „well known port“ (Port von 1 – 1023) zugeordnet? _____

   d. Bestimmen Sie die sog. Sockets (IP-Adresse und Ports) der Verbindung:

      Source: 172.16.15.7

      Destination: 172.16.1.13

   e. Ist der Inhalt der Datenpakete lesbar? Nein

5. Starten Sie Wireshark neu und zeichnen Sie einen ftp-Zugriff auf. Öffnen Sie dazu eine Kommando-Zeile (cli) und starten Sie ftp. Es erscheint der prompt ftp>
   Öffnen Sie nun mit dem Befehl „open 172.16.1.13“ eine Verbindung mit dem ftp-Server. Geben Sie bei der Benutzer-Abfrage ihren Benutzernamen ein. Gegen Sie ihr Passwort ein. Die Anmeldung schlägt fehl. Stoppen Sie Wireshark und filtern Sie nach ftp.

   a. Welche Ports werden für den ftp-Zugriff verwendet? 61050, 21

   b. Suchen Sie das Paket zur Benutzer-Abfrage. Welcher Benutzer wird angezeigt? Sind die Benutzerdaten verschlüsselt? 21ITA007
      Nein

   c. Suchen Sie den Eintrag zur Passwort-Abfrage. Ist das Passwort verschlüsselt?
      Nein