TECHNISCHE UNIVERSITÄT BERLIN
Fakultät IV – Elektrotechnik und Informatik
Fachgebiet Intelligente Netze
Prof. Anja Feldmann, Marco Canini, Petr Kuznetsov, Stefan Schmid
Arne Ludwig, Oliver Hohlfeld, Juhoon Kim, Thomas Krenc, Enric Pujol, Felix Poloczek

8. Blatt: Network Protocols and Architectures, WS 12/13

Aufgabe 1: (15 + 10 + 10 + 15 + 20 + 20 + 10 = 100 Punkte) *Verkehrsanalyse*

Wir widmen uns nun der Analyse von realem Netzververkehr mittels dem Analysewerkzeug Wireshark[1]. Öffne hierzu `u08-trace.pcap`[2] mittels Wireshark. Wireshark bietet eine Fülle von vorgefertigen Analysewerkzeugen. Da es der primäre Zweck des Traces ist, ein erstes Verständnis für die Materie zu erlangen, sollten sie erst Verwendung finden, nachdem das Verständnis dafür erlangt wurde wie das gleiche Ergebnis manuell durch reines Anwenden der Displayfilter erzielt werden kann.

Die nachfolgenden Werkzeuge können sehr hilfreich sein:

- Einen einzelnen Fluss auswählen: Rechtsklick auf ein Paket und *Follow TCP Stream* im Kontextmenü auswählen
- Sequenzdiagramme erstellen: Statistics → Flow Graph → TCP flow → OK

Diese Aufzählung ist jedoch keineswegs vollständig und weitere Werkzeuge können sich bei der Lösung dieser Übung als hilfreich erweisen, sie müssen jedoch nicht zwingend angewendet werden. Des Weiteren wird es äusserst hilfreich sein, Displayfilter definieren zu können. Eine Einführung hierzu ist im Wireshark-Handbuch[3] zu finden.

Wichtig: Hier gilt der Weg ist das Ziel; es ist für die Beantwortung der Fragen *nicht* ausreichend lediglich die Lösung zu nennen. Teil jeder Lösung soll eine nachvollziehbare Beschreibung des Vorgehens sein, mit dem die Ergebnisse produziert wurden. Wenn beispielsweise Displayfilter verwendet wurden, sollen diese auch in der Lösung dokumentiert sein. Diese Beschreibung soll das Vorgehen und die Lösungsidee dokumentieren, z.B. wie und weshalb verschiedene Filter kombiniert wurden.

(a) Wieviele TCP Verbindungen sind im Trace zu erkennen? Zu welchem Zeitpunkt beginnen diese, wann enden sie? Wie kann der Anfang bzw. das Ende einer Verbindung erkannt werden? Sind einige dieser Verbindungen zeitlich parallel zueinander? Gibt es UDP-Flüsse?

Löse diese Aufgabe für einen exemplarischen Fluss unter Verwendung von Displayfiltern (Hinweis: filtere nach Verbindungsflags). Von Wireshark bereitgestellte Automatismen (analyzer) *können* für die verbleibenden Flüsse genutzt werden.

(b) Kannst du Paketverluste in TCP-Flüssen beobachten? Gib ein Beispiel.

(c) Welche Hosts sind im Trace zu erkennen? Welche Dienste bietet jeder dieser Hosts an? Welche Protokolle der Anwendungsschicht können beobachtet werden? Welche der Hosts sind Clients, welche sind Server?

(d) Ermittle aus Informationen, die im Trace enthalten sind, die DNS-Namen der einzelnen Hosts. Zeige für einen Host, wie die Analyse von DNS-Verkehr diesen Namen ergibt. Beschreibe wie die Analyse des DNS-Verkehrs zur Lösung führt. Für alle anderen Hosts kann auf Automatismen in Wireshark zurückgegriffen werden. Welche Hosts haben keinen DNS-Namen?

(e) Versuche zu jeder beobachteten Verbindung folgende Informationen zu ermitteln: i) Was sind die Aktionen des Nutzers / Was wurde angefordert? ii) Welche Informationen liegen im Klartext vor (beispielsweise Passwörter)? Dies wird nicht für alle Flüsse möglich sein. Falls diese Information nicht erhoben werden kann, begründe kurz weshalb dies nicht möglich ist.

[1] `http://www.wireshark.org/`
[2] `https://www.isis.tu-berlin.de/mod/resource/view.php?id=302686`
[3] `http://www.wireshark.org/docs/wsug_html_chunked/ChWorkDisplayFilterSection.html`

(f) Welche Informationen kann man über die Netzwerktopologie durch Analyse des Link Layers ableiten: Der Verkehr wurde in einem LAN aufgezeichnet, welche anderen Hosts befinden sich im gleichen LAN? Hinweis: Filtere nach MAC-Adressen und analysiere deren Verwendung. Bedenke dabei wie diese Adressen in der Adressierung auf dem Link Layer genutzt und wann sie z.B. umgeschrieben werden. Welchen Hosts sind mehrere IP-Adressen zugewiesen?

(g) Analysiere die Pakete 18 bis 20. Welches Anwendungsprotokoll wird hier benutzt? Was ist die Semantik dieser Pakete? Haben sie Auswirkungen auf den späteren Verlauf der Verbindung?

Abgabe bis Donnerstag, den 20. Dezember 2012 nur bis 13:55 h s. t.

- **Als PDF-Dateien (keine MS-Office- oder OpenOffice-Dateien):** Mittels ISIS hochladen (`https://www.isis.tu-berlin.de/course/view.php?id=7028`)
- **In Papierform:** Postfach im Telefunkenhochhaus (Erdgeschoss, hinter dem Pförtner rechts)
- Gib auf deiner Lösung deinen Namen, deine Matrikelnummer **und** den Namen deines Tutors an.