Rechnernetze und Verteilte Systeme: Block 7

**3 Praktische Aufgaben**

Sie haben fur¨ diesen Block 2 Wochen Zeit die Aufgaben zu bearbeiten. Aufgrund des verschobenen ISIS-Test wird keine Rucksprache¨ stattfinden.

Aufgabe 5:

(Abgeleitet aus der Forensics Challenge 14 des Honeynet Project erstellt von Thomas Chopitea and Max-imilian Hils)Damit in einem Netzwerk unterschiedliche Systeme miteinander kommunizieren konnen,¨ mussen¨ mehrere Herausforderungen gelost¨ werden. Dazu gehort¨ z.B. der Zugriff auf das physikalische Medium oder die Wegewahl durch ein komplexes Netzwerk. Die Losung¨ dieser Probleme wird durch entsprechende Protokolle realisiert.

Damit ein neues Protokoll nicht jedes Mal alle Aufgaben vollstandig¨ neu losen¨ muss, sind die Aufgaben in einem Netzwerk auf mehrere Schichten verteilt. In der Regel umfasst jedes Protokoll die Aufgaben einer Schicht und bietet uber¨ definierte Schnittstellen seine Dienste an die daruberliegende¨ Schicht an. Daneben gibt es naturlich¨ auch einige Ausnahmen, bei denen mehrere Schichten abdeckt werden.

In vorhergehenden Terminen haben Sie bereits das TCP und UDP benutzt, um den Transport von Daten zwischen zwei Prozessen uber¨ ein Netzwerk zu ermoglichen¨. Die einzelnen Datagramme der Transport-protokolle werden im Internet mit dem Internet Protocol (IP) transportiert. Beim Senden von TCP oder UDP Daten wird daher vor die UDP oder TCP-Steuerinformationen noch ein IP Header mit IP Steuerin-formationen vorangestellt. Erst beim Empfanger¨ werden diese Informationen in der jeweiligen Schicht wieder vollstandig¨ entfernt und ausgewertet, und die Daten werden an die nachste¨ Schicht weitergegeben. Prinzipiell geschieht dies bei jedem einzelnen verwendeten Protokoll.

In diesem Termin soll das Verstandnis¨ fur¨ die einzelnen Protokolle und deren Funktionsweise vertieft werden. Dazu werden vorgegebene Mitschnitte von Paketubertragungen¨ mit Hilfe von entsprechen-der Software analysiert. Nutzen Sie dafur¨ den freien Network-Analyzer Wireshark[2](#page4). Das Programm decodiert die Datenpakete von gelaufigen¨ Protokollen und stellt den Netzwerkverkehr in einem fur¨ Men-schen lesbaren Format dar. Die einzelnen Funktionen der Software sind auf der zugehorigen¨ Webseite dokumentiert.

Untersuchen Sie den auf der ISIS-Seite bereitgestellten Packet-Trace mit Wireshark.

1. Wie viele Pakete umfasst der Trace?
2. Wie groß sind die Pakete im Durchschnitt?
3. Notieren Sie alle im Trace auftauchenden MAC-Adressen.
4. Wie viele IP-Adressen tauchen im Trace auf?
5. Einige der auftauchenden MAC-Adressen sind mit IP-Adressen verknupft¨. Notieren sie diese Verknupfungen¨.
6. Bei welchem Anteil der Pakete wird das Internet Protocol (IP) auf der Vermittlungs/Netzwerkschicht (ISO/OSI Modell) verwendet?
7. Bei welchem Anteil der Pakete wird das Transmission Control Protocol (TCP) auf der Trans-portschicht verwendet?
8. Notieren Sie alle Protokolle der Applikationsschicht die TCP nutzen.
9. Notieren Sie alle Protokolle der Applikationsschicht die das User Datagram Protocol (UDP) nutzen.
10. Notieren sie alle auftauchenden Protokolle der Vermittlungs/Netzwerkschicht.

* Fur¨ gangige¨ Betriebssysteme verfugbar¨ unter <http://www.wireshark.org>oder unter Linux in der Regel uber¨ die Paketverwaltung

4

Rechnernetze und Verteilte Systeme: Block 7

1. Notieren sie alle auftauchenden Protokolle der Sicherungsschicht.
2. Wie viele Domain Name System (DNS)-Abfragen fanden statt?
3. Wie viele IP-Pakete haben einen “Time-To-Live” (TTL) Wert großer¨ als 200, mit genau 128 und mit genau 64? Versuchen sie, eine Erklarung¨ fur¨ die gefundene Verteilung zu finden.
4. Untersuchen Sie das 16. Paket im Trace genauer:
   1. Wie groß ist der Ethernet-Header?
   2. Wie groß ist der IP-Header?
   3. Wie groß ist das IP-Datagram?
   4. Wie groß ist der TCP-Header?
   5. Wie groß ist das TCP-Segment?
5. Erstellen Sie ein Histogramm uber¨ die Lange¨ der IP-Datagramme. Interpretieren Sie das Ergebnis.
6. Zwischen welchen IP-Adressen werden die meisten Bytes ausgetauscht? Erstellen Sie ein His-togramm uber¨ die Lange¨ dieser IP-Datagramme. Interpretieren Sie das Ergebnis.
7. Zwischen welchen IP-Adressen werden die meisten Pakete ausgetauscht?
8. Bestand eine verschlusselte¨ Verbindung? Notieren Sie ggf. die beteiligten Hosts.
9. Wurde ein Web-Browser benutzt? Wenn ja, welche?

Tragen Sie Ihre Antworten in einen PDF-Dokument zusammen und reichen Sie dieses in einer Datei mit dem Namen Block7a.TXXGYY.tar.gz bis Sonntag nach dem zweiten Termin 23:55 Uhr auf ISIS ein.[3](#page5)

* Kleine Eselsbrucke¨ fur¨ alle die immer noch unkomprimierte Tar-Archive abgeben: tar -czvf == “tar compress ze vu\*\*ing files”

5

Rechnernetze und Verteilte Systeme: Block 7