HOCHSCHULE KONSTANZ TECHNIK, WIRTSCHAFT UND GESTALTUNG (HTWG)
Fakultät Informatik
Rechner- und Kommunikationsnetze
Prof. Dr. Dirk Staehle

Vorlesung Rechnernetze
AIN 5

Laborübung

Socket Monitoring

Prof. Dr. Dirk Staehle

Die Abgabe erfolgt durch Hochladen der bearbeiteten Word-Datei in Moodle.

Bearbeitung in Zweier-Teams

Team-Mitglied 1: Alexander Schapelt

Team-Mitglied 2: Josef Müller

Team-Mitglied 3: Walter Vötsch Cortés

1 Einleitung

In diesem Laborversuch lernen Sie, wie Sie eine Übersicht bekommen, mit welchen Rechnern im Internet Anwendungen auf ihrem PC kommunizieren. Die gängigen Betriebssysteme stellen das Tool „netstat“ zur Anzeige der geöffneten Sockets zur Verfügung. Eine komfortablere Anzeige bietet unter Windows z.B. das freie Tool „CurrPorts“ von NirSoft (https://www.nirsoft.net) und unter Linux NetActView (http://netactview.sourceforge.net/download.html, Achtung: weder geladen noch getestet, Download auf eigenes Risiko).

Verwenden Sie für diese Übung wenn möglich ihrem privaten Laptop/PC und nicht den Labor-PC. Eine Analyse der geöffneten Sockets ihres privaten PCs ist für Sie vermutlich interessanter. Achten Sie bei der Arbeit im Team darauf, dass hier Informationen über ihren privaten PC sichtbar werden. Wenn Sie das nicht möchten, sollte jedes Team-Mitglied die Übung selbständig durchführen.

2 Monitoring von Sockets

In diesem Versuch sollen Sie analysieren, mit wem ihr PC kommuniziert und welche Prozesse bzw. Programme für diese Kommunikation verantwortlich sind. Erstellen Sie dazu eine Liste der Programme, die Sockets geöffnet haben und finden Sie heraus, mit wem diese Programme kommunizieren. Nutzen Sie hierzu bevorzugt CurrPorts. In CurrPorts lässt sich unter Options einstellen, welche Sockets angezeigt werden. Machen Sie davon Gebrauch, um die gewünschten Ports darzustellen.

Beantworten Sie die folgenden Fragen:

1) Wie viele Sockets sind insgesamt geöffnet?

   189 Total Ports (unten links in CurrPorts zu sehen)

2) Wie unterscheiden sich die Einträge von TCP und UDP Sockets?
   (Vorgriff auf Kapitel 4.2 der Vorlesung)

TCP Sockets (gesicherte Datenübertragung)	**UDP Sockets** (ungesicherte Übertragung von Datagrammen)
- teils Remote Port und Remote Port Name Eintrag - teils Remote Adresse - hat ein State Eintrag	- kein Remote Port (Standard Ports) und Remote Port Name Eintrag - keine Remote Adresse - stateless

3) Was bedeuten die Einträge in der Spalte „State“ bei TCP Sockets?
(Vorgriff auf Kapitel 4.3 der Vorlesung)
Infos in der Vorlesung oder z.B. hier (eher willkürliche Auswahl):
   a) https://www.computerweekly.com/de/tipp/Netzwerk-Analyse-mit-Netstat-So-finden-Sie-offene-Ports-und-Malware
   b) https://www.ibm.com/support/knowledgecenter/SSLTBW_2.1.0/com.ibm.zos.v2r1.halu101/constatus.htm
   c) https://de.wikipedia.org/wiki/Transmission_Control_Protocol

   Die Spalte „State“ zeigt, in welchem Status sich die Verbindung befindet oder um welche Art es sich handelt.

State	**Bedeutung**
abhören / listening	- zeigt einen klassischen offenen Port, der für eingehende Verbindungen bereit ist
hergestellt / established	- bedeutet, dass tatsächlich eine Verbindung zwischen Ihrem Rechner und einer Remote-IP-Adresse samt dazugehörigem Port besteht - hier findet eine Datenübertragung statt
schliessen_warten / close wait	- aktive Verbindung wird in diesem Status beendet

4) Wie viele Server Ports hat ihr Rechner geöffnet (state=Listening)? Auf diesen Ports (und den UDP Ports) kann ihr Rechner von außen kontaktiert werden.

   37 TCP Listening + 45 UDP = 82

5) Wie viele Sockets (ESTABLISHED) werden neu geöffnet, wenn Sie die Messung nach einer Minute erneut durchführen bzw. die Ergebnisse aktualisieren?
(In CurrPorts AutoRefresh ausschalten und einen manuellen Refresh durchführen)

   2

6) Sehen Sie zahlreiche Sockets mit IP-Adresse 127.0.0.1? Finden Sie heraus, wofür diese IP Adresse benutzt wird und blenden Sie alle Sockets mit dieser Adresse aus.

Bei dem localhost oder der IPv4 Adresse 127.0.0.1 handelt es sich um einen als Standard definierten Domainnamen, der auf den eigenen Computer oder Server verweist. Damit können Computerprogramme innerhalb eines Rechners miteinander kommunizieren und das Internet-Protokoll als universeller Standard benutzen.

7) Bestimmen sie anhand der Portnummer und der Portliste für einige interessante/unbekannte Prozesse, mit welchem Protokoll diese kommunizieren. Die Zuweisung von Portnummer zu Protokollen finden Sie z.B. hier:
   a) Offiziell (IANA): https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.txt
   b) Wikipedia: http://de.wikipedia.org/wiki/Liste_der_standardisierten_Ports
   c) Häufigste Dienste: https://isc.sans.edu//services.html

Portnummer	**Protokoll**
5353	- UDP - Beschreibung: Multicast DNS (mDNS) - Status: offiziel
843	- TCP - Beschreibung: Adobe Flash socket policy server - Status: inoffiziell
57621	- UDP - Beschreibung: Spotify - Status: inoffiziell

3 Details über die Kommunikationspartner ihres PCs

Das Tool „IPNetInfo“ von NirSoft dient dazu, die zu einer IP Adresse öffentlich verfügbare Information abzurufen und darzustellen. Nachdem Sie IPNetInfo gestartet haben, können Sie es direkt aus CurrPorts aufrufen. Markieren Sie dazu einen oder mehrere Sockets und clicken Sie die rechte Maustaste oder drücken Ctrl+I. Unter Linux habe ich leider kein komfortables Tool gefunden. Sie können entweder den Befehl „whois“ verwenden oder eine Web-Seite nutzen, auf der Sie einzelne IP-Adressen eingeben können.

Analysieren Sie jetzt, mit welchen Servern/Rechnern die Prozesse auf ihrem PC kommunizieren. Generieren Sie dazu mit Hilfe von IPnetInfo in Excel eine Gesamtübersicht der Kommunikationspartner ihres Rechners.

1) Finden Sie über WireShark heraus, wie das Programm „IPnetInfo“ die Informationen erhält. Welcher Server wird kontaktiert? Welches Protokoll wird verwendet?

   - durchsucht einen Whois-Server
   - Whois Protokoll wird verwendet (Datenbanksystem)

2) In welchem Netz befindet sich der Web-Server, der in der ersten WireShark-Aufgabe aufgerufenen Web-Seite?
   - Netz: DE-LINK11-20111007

3) Welche Informationen finden Sie über die HTWG?

```
inetnum:       141.37.0.0 - 141.37.255.255
netname:       FH-KN
country:       DE
admin-c:       HKTW1-RIPE
tech-c:        HKTW1-RIPE
org:           ORG-HKTW1-RIPE
status:        LEGACY
remarks:       ************************************************
remarks:       * DEFAULT ABUSE CONTACT: abuse@htwg-konstanz.de  *
remarks:       ************************************************
mnt-by:        BELWUE-MNT
mnt-by:        RIPE-NCC-LEGACY-MNT
created:       2002-04-25T09:54:38Z
last-modified:  2016-04-14T08:23:18Z
source:        RIPE
sponsoring-org: ORG-BA9-RIPE

organisation:   ORG-HKTW1-RIPE
org-name:       Hochschule Konstanz Technik, Wirtschaft und Gestaltung
org-type:       OTHER
address:        Brauneggerstr. 55
```

address: 78462 Konstanz, Germany
e-mail: netzwerk@htwg-konstanz.de
admin-c: HKTW1-RIPE
tech-c: HKTW1-RIPE
abuse-c: HKTW1-RIPE
mnt-ref: BELWUE-MNT
mnt-by: BELWUE-MNT
created: 2015-06-17T14:46:25Z
last-modified: 2015-06-18T11:34:36Z
source: RIPE

role: Hochschule Konstanz Technik, Wirtschaft und Gestaltung
address: Brauneggerstr. 55
address: 78462 Konstanz, Germany
e-mail: netzwerk@htwg-konstanz.de
admin-c: MS3208-RIPE
tech-c: MS3208-RIPE
nic-hdl: HKTW1-RIPE
abuse-mailbox: abuse@htwg-konstanz.de
mnt-by: BELWUE-MNT
created: 2015-06-17T14:46:25Z
last-modified: 2015-06-18T11:34:36Z
source: RIPE

% Information related to '141.37.0.0/16AS553'

route: 141.37.0.0/16
descr: FH-KONSTANZ
origin: AS553
mnt-by: BELWUE-MNT
created: 1970-01-01T00:00:00Z
last-modified: 2001-09-22T09:32:38Z
source: RIPE

4 Sockets beim Laden einer Web-Seite

In der WireShark-Übung haben Sie bereits herausgefunden, wie Sie die Anzahl der geöffneten Sockets beim Download einer Web-Seite wie z.B. www.spiegel.de feststellen können.

Mit CurrPorts geht das jetzt einfacher und mit mehr Informationen. Sie können die Sockets auch direkt dem Prozess (ihrem Browser) zuordnen und Informationen über die Remote IP-Adresse erhalten.

1) Bestimmen Sie die Anzahl Sockets, die geöffnet werden, wenn Sie www.spiegel.de herunterladen.
   a) Wenn es Sie interessiert: vergleichen Sie die Anzahl der Sockets mit und ohne Ad-Blocker

Anzahl Sockets mit Ad-Blocker	**Anzahl Sockets ohne Ad-Blocker**
8	26

2) Was ist die maximale Anzahl von Sockets pro Remote-IP-Adresse?

   Pro Adresse kann man 65535 Ports öffnen -> maximal 65535 Sockets pro Remote-IP-Adresse

3) Welche Remote-Ports werden verwendet?

   80 und 443

4) Wie viele verschiedenen Firmen können Sie die Remote-Hosts zuordnen (am Besten über Contact Name in IPNetInfo)?

   Amazon, Mini, Hetzner Online GmbH, Akamai Technologies, Google, Verizon, 1blu, Wikimedia, Microsoft, McAfee, Apple

5) Laden Sie eine andere populäre Web-Seite und vergleichen Sie die Liste der kontaktierten Firmen.

   https://www.t-online.de/

   Amazon, Verizon, Hetzner Online GmbH, Google, Ströer Group …