Übungsblatt 04 – Wireshark

Aufgabe A – TCP: 3-Way-Handshake

Nachdem Sie sich bereits theoretisch mit dem 3-Way-Handshake auseinandergesetzt haben, sollen Sie nun schauen, ob der TCP-Handshake tatsächlich wie theoretisch beschrieben arbeitet.

1. Überlegen Sie sich eine Anfragen an eine Website (dies sollte TCP nutzen, wie HTTP!), die Sie noch nicht von der VM aus getätigt haben. Da ansonsten bestimmte Inhalte bereits gecacht vorliegen könnten oder über andere Verfahren eine TCP-Handshake vereiteln könnten.
2. Starten Sie Wireshark, richten Sie Interface und Protokoll-Type ein. Filtern Sie nur auf eine speziellen Request!
3. Lösen Sie den Handshake durch aufrufen der Website (oder Ressource) aus, während Wireshark den Netzverkehr mitschneidet.
4. Analysieren Sie den 3-Way-Handshake!
5. Zum Vergleich: Analysieren Sie ihren Mitschnitt mit folgender Aufzeichnung: https://wiki.wireshark.org/TCP_3_way_handshaking?action=AttachFile&do=view&target=3-way+handshake.pcap

Aufgabe B – ICMP

Da die Befehle *ping* und *traceroute ICMP* nutzen, sollen Sie mit Wireshark solche Request mitverfolgen.

1. Setzen Sie alle notwendigen Parameter um Wireshark mitlaufen zu lassen, sodass Sie die ICMP-Nachrichten mitverfolgen können.
2. Pingen Sie einen Rechner mit seinem Namen an (bspw.: `mi.fu-berlin.de`).
3. Ping auf eine IP-Adresse (bspw.: 160.45.117.199).
4. Ping auf die IP-Adresse Ihres Routers.
   Hinweis: Sie können diese durch *ip r* oder *route* in Erfahrung bringen.

```
ip r
default via XXX.XXX.XXX dev DEVICE proto dhcp src YOU.RIP.ADD metric VALUE
#or
route -n
Destination  Gateway  Genmask  Flags  Metric  Ref  Use  Iface
0.0.0.0  XXX.XXX.XXX  0.0.0.0  UG  VALUE  0  0  DEVICE
```

5. Ping auf meine eigene IP-Adresse.
6. Ping auf die Loopback-Adresse.
7. Starten Sie eine Routenverfolgung via *traceroute* auf eine beliebige Adresse. Verfolgen Sie dabei den Ausgabe auf der Konsole als auch in Wireshark (Filtern Sie in Wireshark entsprechend). Spiegeln sich die Einträge in Wireshark mit denen auf der Kommandozeile?
8. Erläutern Sie die Ergebnisse Ihrer vorigen Aufgabe. Wie funktioniert *traceroute* und wie hängt dies mit *ICMP* zusammen?

Aufgabe C – Routing & Traceroute

Nachdem Sie recherchiert haben, wie *traceroute* arbeitet, welche Kritik an Traceroute geäußert wurde und wie diese mit dem Tool Paris-Traceroute abgestellt wurden, sollen beide Tools hier kurz erprobt werden.

1. Überlegen Sie sich zunächst anhand Ihrer Recherche was *traceroute* in etwa ausgeben müsste, wenn Sie im Labor eine Route von einem Rechner A zu einem Rechner B verfolgen würden. Wobei beide Rechner zu unterschiedlichen Netzwerken gehören (d.h. unterschiedlichen Tischreihen).
2. Nutzen Sie anschließend *traceroute* um sich die Router zwischen zwei Laborrechnern anzeigen zu lassen. Stimmen Ihre theoretische Überlegungen mit denen von *traceroute* überein? Falls nicht, sollten Sie analysieren woran dies liegen könnte.
3. Vergleichen Sie die Ausgaben von *traceroute* und *paris-traceroute* für folgende IP-Adressen:
   a) 41.231.21.44
   b) 91.198.174.192
   c) 37.220.21.130
   d) 80.239.142.229

   Hinweis: Für *paris-traceroute* sollten Sie den „exhaustive algorithm“ Nutzen (in machen Versionen als Parameter: `-na exhaustive`)
4. Analysieren Sie anschließend die Ausgabe beider Tools.
5. Warum wurde Ihnen eine Liste von IP-Adressen genannt anstelle von Domainnamen? Nennen Sie mindestens zwei Gründe!

Aufgabe D - Unencrypted Password Sniffing

Für diese Aufgabe benötigen Sie das Setup aus der vorigen Übung, in der drei Rechner miteinander verbunden sind. Jedoch soll für diese Aufgabe der Router kein Headless-System sein (Linux ohne GUI), sondern das Debian mit grafischer Oberfläche. So haben Sie Zugriff auf Wireshark.
Folgendes Szenario soll umgesetzt werden:
Zwei Rechner kommunizieren via HTTP miteinander (HTTP Request). Die Kommunikation erfolgt über einen Router (statisch), der von Ihnen kontrolliert wird. Also Sicherheitsmaßnahme wird auf dem Webserver eine grundlegende Authentisierung via Passwort eingerichtet. Unbefugte können also nicht auf die Inhalt der Website zugreifen.
Da jedoch keine kryptografischen Verfahren angewandt werden, kann das Passwort in Erfahrung gebracht werden.

1. Um das Passwort-Sniffing etwas zu erleichtern, soll der Netzwerkverkehr über einen neugierigen Router erfolgen. Passen Sie die Routing-Tabelle und das Forwarding wie folgt an:
   - Beide Host kommunizieren über den Router, müssen diesen also als Default-Gateway eingestellt haben.
   - Richten Sie den Router entsprechend ein. Sodass dieser den Verkehr weiterleitet.

2. Der Apache Webserver liefert Ihnen nur die Default-Seite (s. zweiter Übungsblatt).
   a) Nehmen Sie für die Konfiguration des Webservers ein Backup vor! Alle Dateien die Sie ändern müssen, sollen zuvor gesichert werden. Kopieren Sie entsprechend die Dateien mit den Ihnen bekannten Kommandozeilenbefehlen im gleichen Ordner. Folglich sollen sich im gleichen Ordner die Backups wie auch die Originaldateien befinden.
   Die Kopie kann beispielsweise die Dateiendung *.bck* tragen. [1]
   b) Nicht jeder Nutzer soll auf den Inhalt Ihrer Webseite zugreifen dürfen, daher soll eine einfache Passwortabfrage den Inhalt Ihrer Website sichern.
   Richten Sie eine Passwortauthentifizierung ein, die auf dem Webserver *A* dem Nutzer `web` und auf Webserver *B* dem User `bew` Zugriff gewährt. Allen anderen Nutzern soll kein Zugriff erlaubt sein!

3. Als Hilfestellung für den Webserver können Sie wie folgt vorgehen:
   - Die Passwortauthentifizierung kann mithilfe des Kommandos *htpasswd* eingeleitet werden.

   ```
   1 sudo htpasswd -c /etc/apache2/.htpasswd YOURUSERNAME
   ```

   - Anschließend kann in der Datei `/etc/apache2/apache2.conf` entsprechend der Inhalt Ihrer Website geschützt werden.

[1] Es gibt anschließend also eine `/etc/apache2/apache2.conf` und eine `/etc/apache2/apache2.conf.bck` Datei.

```
<Directory "/var/www/html">
  AuthType Basic
  AuthName "Speak, friend and enter"
  AuthUserFile "/etc/apache2/.htpasswd"
  Require user YOURUSERNAME

  Order allow,deny
  Allow from all
</Directory>
```

- Testen Sie ob Ihre Konfiguration korrekt ist (*apachectl* ist Ihr Helfer)

4. Der Administrator des Sniffers ist überaus neugierig und soll die verwendeten Nutzernamen/Passwort Kombinationen ausschließlich durch Analyse des Netzwerkverkehrs in Erfahrung bringen. [2]
   a) Analysieren Sie den Traffic! Nach welchem Protokoll müssen Sie suchen?
   b) Stellen Sie entsprechen den Filter in Wireshark ein.
   c) Finden Sie das Tupel aus Nutzernamen und Passwort.
   Wie können Sie im gesamten Verkehr noch weiter filtern, sodass Sie das Paket mitsamt Nutzernamen und Passwort finden?
   Hinweis: Es kann passieren, dass der Browser die Website im Zwischenspeicher behält (cached), sodass Ressourcen gespart werden können. Möglicherweise müssen Sie entsprechend den Browser-Cache leeren, bevor Sie Änderungen im Browser sehen können.

Aufgabe D - Bestimmung des physischen Rechners zu einer IP-Adresse – ARP

Sie haben bereits theoretisch recherchiert wie die Zuordnung von physischer Adresse zu einer IP-Adresse vonstatten geht. Im Folgenden sollen Sie herausfinden, ob die Auflösung von IP-Adresse auf physische Adresse wirklich analog zu Ihren theoretischen Recherchen abläuft.

1. Finden Sie mithilfe Wiresharks heraus, wie die Adressauflösung funktioniert.
   a) Leeren Sie zunächst den ARP-Cache.
   b) Pingen Sie nun einen Rechner an, den Sie vorhin noch nicht „angepingt“ haben. Die dafür ausgetauschten Pakete (und wahrscheinlich einige mehr) werden „gesnifft“.

[2] Dieses Szenario ist sehr fingiert, soll aber nur verdeutlichen, dass ohne Schutz unverschlüsselte Daten leicht einsehbar sind! Dies ist auch der Fall, wenn Daten nicht direkt über einen Rechner gehen – s. Promiscous-Mode oder im WiFi-Verkehr

c) Beenden sie das Mitschneiden des Netzwerksverkehrs und setzen Sie als Filtern die MAC-Adresse ihres Adapters.

d) Versuchen Sie über den Mitschnitt herauszufinden, wie die Bestimmung des zugehörigen Netzadapters und die MAC-Adresse erfolgt.

1)

2. Damit Ihr Rechner nicht jedes mal eine Auflösung veranlassen muss, werden die ARP-Informationen lokal in einem Cache zwischengespeichert („cached“).

   a) Lassen Sie sich Ihren aktuellen ARP-Cache anzeigen. Welche Informationen können Sie diesem entnehmen?

   b) Schauen Sie kurz nach wie lange der ARP-Cache Einträge vorhält.

   c) Lassen Sie zwei VMs die IP-Adressen tauschen. Dies sollte möglichst schnell umgesetzt werden!

   d) Versuchen Sie nun durch eine dritte VM eine „alte“ IP-Adresse zu erreichen. Werden die Daten an den richtigen Knoten übermittelt?

   e) Verfolgen Sie die Datenübermittlung per Wireshark mit.

Fakultativ: Aufgabe E - Packet Analysis

Im Moodle-Kurs liegt eine Zip-Datei `network_packets.zip`. Diese enthält verschiedene Dateien die Sie auf verschiedene Arten in Wireshark öffnen können. Sie sollen diese Pakete analysieren. Teilweise sind in diesen Paketen Passwörter und Zugangsdaten zu finden, in einigen Fällen können ganze Nachrichten oder Geräte Informationen analysiert werden.

1. Die Datei `ch1.pcap` ist eine FTP-Session mit Passwort Authentifizierung. Finden Sie das Paket sowie Passwort.

2. Die Datei `ch2.pcap` ist eine Telnet-Session mit Passwort Authentifizierung. Finden Sie das Paket sowie Passwort.

3. Die Datei `raw_ethernet_frame` ist ein Ethernet Frame in Hex-Format. Das heißt, Sie müssen einen Hex-Dump auswerten. Finden Sie heraus, was im Ethernet-Frame enthalten ist.

4. Die Datei `ch3.pcap` ist eine Twitter-Session welche die Authentifizierung entält. Finden Sie heraus, wie diese umgesetzt wurde und finden Sie das Passwort.

5. Die Datei `ch18.bin` für die Authentisierung von Bluetooth-Geräten gedacht. Im wesentlichen benötigen Sie die MAC-Adresse des Gerätes und den Gerätenamen. Beides ist in der Datei enthalten. Die Authentisierung erfolgt die Hashing mit SHA1

(eine kryptografische Hashfunktion [3]). Finden Sie das Tupel aus MAC-Adresse und Gerätenamen heraus und lassen Sie die SHA1 Funktion darüber laufen.

```
1 echo "XXXXXXXXXXXXXXXXXXX" | sha1sum
```

[3] Mehr dazu demnächst. SHA1 gilt seit Jahren als unsicher!