

Übungsblatt 05 – Wireshark

Hilfreiche Tools:

- netstat, ss
- ip neigh
- arp -d
- arp
- ip -s -s neigh flush all
-

Aufgabe A - Setup & Wireshark 101

Nachdem im theoretischen Teil mithilfe der Tutorials, sowie Ihrer Recherche die Grundlagen für die Nutzung von Wireshark gelegt haben, sollen Sie dieses Wissen nun anwenden.

- 1.) Schalten Sie zunächst, wenn nicht bereits geschehen, das DHCP aus! Setzen Sie anschließend das Netzwerk wie in der vorigen Übung mit den Ihnen bekannten Tools um. Halten Sie dabei das gewohnte Adressschema ein:

Tabelle 1: Adressschema für das Labor

	IP IP-Range
LAN_X	10.0.X.Y/Size
Backbone	10.10.10.100 + ρ
Labornetz	10.0.0.0/8
Uplink	10.10.10.254
DNS	10.10.10.254

- 2.) Ist Ihr Netzwerk soweit Einsatzbereit? Nutzen Sie die Tools *ip*, *ifconfig*, *ss* und *netstat* um die nachfolgenden Fragen zu beantworten.
 - a.) Haben Ihre Hosts die richtigen IP-Adressen?
 - b.) Können Sie andere Rechner im Labornetzwerk erreichen?
 - c.) Ist Ihr Uplink funktionstüchtig? D.h. haben Sie Zugang ins Internet?
 - d.) Funktioniert Ihre Namensauflösung? M.a.W. können Sie Hosts anhand ihrer Namen auflösen?

Falls einer die oben genannten Punkte nicht erfüllt, sollten Sie dies abstellen. Dazu können Sie eine manuelle Konfiguration vornehmen (Übung 3 & 4).

- 3.) Überprüfen Sie, ob Ihr Nutzer der Gruppe *wireshark* angehört. ¹

¹Sollte dies nicht der Fall sein, müssen Sie dies vornehmen. Das Tool *adduser* bzw. *usermod* kann dies vornehmen.

- 4.) Starten Sie Wireshark (wenn Sie möchten können Sie Wireshark auch in der Shell ausführen). Finden Sie sich zurecht! Wiresharks grafische Oberfläche sollte im wesentlich dem entsprechen, was Sie in den Tutorials gesehen haben. Finden Sie die Eingabemaske für das Capturing. Für alle nachfolgenden Aufgaben sollen die Mitschnitte auf dem Interface *eth0* vorgenommen werden.
- 5.) Erzeugen Sie Traffic (beispielsweise durch Nutzung des Browsers).
- 6.) Analysieren Sie den eben aufgenommenen Mitschnitt, sodass Ihnen der Workflow mit Wireshark vertrauter wird.
 - Welche Pakete treffen Sie sehr häufig an?
 - Wenden Sie einige Filter aus den Hausaufgaben auf Ihren Traffic an (Filtern nach Protokoll, IP, MAC,...).

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

Mit dem zweiten Übungsblatt haben Sie ein geswitchtes Netzwerk umgesetzt. Wie schon angesprochen sind Switches jedoch Link-Layer-Devices und kommen ohne IP-Adressen aus. Dennoch mussten Sie IP-Adressen konfigurieren. 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 in Wireshark heraus, wie die Adressauflösung funktioniert.
 - (i) Leeren Sie zunächst den ARP-Cache.
 - (ii) Pingen Sie nun einen Rechner an, den Sie vorhin noch nicht „angepingt“ haben. Die dafür ausgetauschten Pakete (und wahrscheinlich einige mehr) werden „gesniff“.
 - (iii) Beenden sie das Mitschneiden des Netzwerkverkehrs und setzen Sie als Filtern die MAC-Adresse ihres Adapters.
 - (iv) Versuchen Sie über den Mitschnitt herauszufinden, wie die Bestimmung des zugehörigen Netzadapters und die MAC-Adresse erfolgt.
- 2.) Damit Ihr Rechner nicht jedes mal diese Daten abfragen muss, werden diese Informationen lokal in einem Cache zwischengespeichert („gecacht“).
 - a.) Mit welchem Programm können Sie sich den ARP-Cache anzeigen lassen?

b.) Lassen Sie zwei Raspberry Pis die IP-Adressen tauschen. Benutzen sie die Kommandozeile, sodass Sie dies anschließend wieder rückgängig machen könne. Wann und wie kann ein dritter Raspberry Pi die beiden nun „anpingen“?

Aufgabe C - ARP-Cache-Poisoning

Wie in den Hausaufgaben bereits zu erahnen war, dürfen Sie nun ein wenig Unruhe in Ihren Netzwerken stiften!

Sie sollen in diesem Teil der Laborübung ein ARP-Spoofing des Routers übernehmen. Um dies zu erreichen, sollen Sie den ARP-Cache so manipulieren, sodass sämtlicher Verkehr zwischen Ihren LANs *A* und *B* nicht mehr über den Router geleitet wird, sondern über den Angreifenden Host.

- 1.) Zunächst müssen Sie Angreifen und Opfer in Ihren Netzwerk auswählen. Die sollte weder der Router, noch der Backbone-Router sein. Vermerken Sie sich entsprechend die IP-Adressen.
- 2.) Analysieren Sie den ARP-Cache des anzugreifenden Systems.
- 3.) Da der angreifende Host als MITM-Router fungiert, muss auch hier das Routing aktiviert sein und eine Default-Route zum Backbone angelegt werden, sodass der Abgefangene Traffic auch beim Ziel ankommt.
- 4.) Im Ordner `~/arp_poison/` liegt ein Python-Skript, welche für den Angriff genutzt werden kann. Bevor Sie dies einsetzen: Schauen Sie sich das Skript erneut an. Wie muss dieses Skript ausgeführt werden?
- 5.) Führen Sie das ARP-Cache-Poisoning mithilfe des Python-Skripts durch. Lassen Sie sowohl auf dem angreifenden als auch angegriffenen System Wireshark mitlaufen.
- 6.) Betrachten Sie den ARP-Cache während des Angriffs, sowie einige Zeit nachdem Angriff.
- 7.) Ziehen Sie ein Fazit aus dem eben durchgeführten Angriff!

Aufgabe D - Unencrypted Password Sniffing

Nachdem Sie nun auch praktisch mit Wireshark Ihre ersten Erfahrungen gesammelt haben, sollen Sie mithilfe des Sniffers Passwörter im unverschlüsselte Traffic „dumpen“. Dazu ist ein kleines Setup notwendig. Ihr Netzwerk sollte nach Möglichkeiten aus zwei Subnetzen sowie einem Router bestehen. In jedem Subnetz soll ein Webserver aufgesetzt werden.

- 1.) Pro Bankreihe sollen je zwei Apache Webserver aufgesetzt werden, pro Subnetz je ein Webserver.
Der Apache Webserver liefert Ihnen eine Default-Seite. Für diese Übung reicht dies aus.
- 2.) 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 im Subnetz A dem Nutzer *web* und im Subnetz B dem User *bew* Zugriff gewährt und allen anderen Nutzern kein Zugriff erlaubt.
- 3.) Nehmen Sie für die Konfiguration des Webserver ein Backup vor! D.h. alle Dateien die Sie ändern müssen, sollen zuvor gesichert werden. Kopieren Sie entsprechend die Dateien, mit den Ihnen bekannten Kommandozeilenbefehlen im gleichen Ordner, sodass sich im gleichen Ordner die Originaldatei, als auch eine Kopie befindet. Die Kopie kann beispielsweise die Dateiendung *.bck* tragen.²
- 4.) Als Hilfestellung für den Webserver können Sie wie folgt vorgehen:

- Für das Binding des Webserver muss in der Apache Konfiguration (s. */etc/apache2/apache2.conf*) die IP-Adresse und optional der Port mit dem Befehl *Listen* gesetzt werden.

```
1 Listen IP:Port
```

- 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 <Directory "/var/www/html">
2   AuthType Basic
3   AuthName "Speak, friend and enter"
4   AuthUserFile "/etc/apache2/.htpasswd"
5   Require user YOURUSERNAME
6
7   Order allow,deny
8   Allow from all
9 </Directory>
```

²Es gibt anschließend also eine */etc/apache2/apache2.conf* und eine */etc/apache2/apache2.conf.bck* Datei.

- Mit dem Tool *apachectl* kann die Konfiguration des Webservers überprüft und anschließend der Apache hochgefahren werden.

```
1 sudo apachectl configtest
2 sudo apachectl start
```

- 5.) Der Administrator des Routers ist überaus neugierig und soll die verwendeten Nutzernamen/Passwort Kombinationen ausschließlich durch Analyse des Netzwerkverkehrs in Erfahrung bringen.
- a.) Analysieren Sie den Traffic – In welchem Protokoll müssen Sie suchen?
 - b.) Stellen Sie entsprechen den Filter in Wireshark ein.
 - c.) Wie könne Sie im gesamten Traffic noch weiter filtern, sodass Sie das Paket mitsamt Nutzernamen und Passwort finden?

System Reset

- 1.) **Sofern Sie keine eigene SD-Karte nutzen:** Setzen Sie die Einstellungen des Raspberry Pis bzw. des Betriebssystems zurück die Sie vorgenommen haben! D.h. setzen Sie das Betriebssystem auf den *dhcpcd* zurück, nehmen Sie alle vorgenommen Änderungen zurück.
- 2.) Nehmen Sie alle vorgenommen Einstellungen zurück. D.h. schalten Sie den Apache-Webserver aus, stellen Sie **alle** ursprünglichen Konfigurationen wieder her. Haken Sie zumindest folgende Liste ab:
 - Eigene IP-Config:
 - `/etc/network/interfaces`
 - Routing/Forwarding:
 - Alle persistenten Routen gelöscht?
 - Forwarding aktiviert? (on the fly oder persistent?)
 - `/etc/sysctl.conf`
 - `/proc/sys/net/ipv4/ip_forward`
 - DNS
 - DNS Einträge verändert?
 - `/etc/resolv.conf`
 - Apache
 - Ist der Apache *disabled*
 - Haben Sie die `/etc/apache2/apache2.conf` zurückgesetzt?

- Haben Sie die `/etc/apache2/.htpasswd` gelöscht?
- `apachectl configtest` aufgeführt?