Übungsblatt 04 – Wireshark

Aufgabe A - Setup & Wireshark 101

Nachdem Sie mithilfe der Hausaufgaben das theoretische Fundament 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 Ihn bekannten Tools um. Sie müssen kein *IPv6* umsetzen!
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 die anderen Knoten innerhalb Ihres Netzes erreichen?
- **c.)** Können Sie andere Rechner im Labornetzwerk erreichen?
- **d.)** Ist Ihr Uplink funktionstüchtig?
- **e.)** Funktioniert Ihre Namensauflösung?

Falls einer die oben genannten Punkte nicht erfüllt ist, sollten Sie dies abstellen, da Sie sonst die restlichen Aufgaben nicht lösen können.

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

4.) Starten Sie Wireshark und 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.

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

5.) Erzeugen Sie Traffic (beispielsweise durch Nutzung des Browsers).

6.) Analysieren Sie den eben aufgenommenen Mitschnitt, sodass Ihnen der Workflow mit Wireshark vertrauter wird.

a.) Welche Pakete treffen Sie sehr häufig an?

b.) Wenden Sie einige Filter aus den Hausaufgaben auf Ihren Traffic an: Filtern nach Protokoll, IP-Adress, 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 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“.

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.

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

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 Daten vorhält.

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

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

e.) Verfolgen Sie die Datenübermittlung per Wireshark mit.

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 das 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. Der Angreifer sollte weder der Router, noch der Backbone-Router sein. Das Opfer ist entweder der Backbone-Router oder der kleine Router. 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 (C, Perl ebenso), 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 Skripts durch.

6.) Lassen Sie sowohl auf dem angreifenden als auch angegriffenen System Wireshark mitlaufen.

7.) Betrachten Sie den ARP-Cache während des Angriffs, sowie einige Zeit nachdem Angriff.

8.) 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.

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.

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. [2]

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 im Subnetz A dem Nutzer `web` und im Subnetz B dem User `bew` Zugriff gewährt. Allen anderen Nutzern soll kein Zugriff erlaubt sein!

2.) Als Hilfestellung für den Webserver können Sie wie folgt vorgehen:

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

```
Listen IP:Port
```

- Die Passwortauthentifizierung kann mithilfe des Kommandos *htpasswd* eingeleitet werden.

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

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

```
<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>
```

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

```
sudo apachectl configtest
sudo apachectl start
```

3.) 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! 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 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:

- 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?