Praktikum zur „IT-Sicherheit“

Aufgabenblatt 2

Sniffer-Tools: Wireshark

Die Aufgaben im Praktikum beschäftigen sich mit Wireshark zur Analyse von Netzwerkdatenverkehr.

Generelle Hinweise zum Aufgabenblatt:

Dokumentieren Sie die Lösungen Ihrer bearbeiteten Aufgaben für das Praktikumsgespräch und Ihre Unterlagen. Es ist sinnvoll, dies elektronisch zu tun, um auch Snapshots bzw. Ausgaben von der Kommandozeile einfach einbinden zu können.

Hinweise zur Vorbereitung: Informationen zu diesem Aufgabenblatt finden Sie beispielsweise unter

http://www.easy-network.de/sniffer.html

http://de.wikipedia.org/wiki/Sniffer

http://de.wikipedia.org/wiki/Wireshark

http://de.wikipedia.org/wiki/IP-Adresse

https://www.wireshark.org/docs/wsug_html_chunked/ChWorkBuildDisplayFilterSection.html

https://gitlab.com/wireshark/wireshark/-/wikis/DisplayFilters

Empfohlene Software:

- VNC-Client
  - Linux:
    remmina z.B. Debian: apt-get install remmina

    tigervnc-viewer z.B. Debian: apt-get install tigervnc-viewer
  - macOS: RealVNC
    https://www.realvnc.com/de/connect/download/vnc/
  - Windows: RealVNC

    https://www.realvnc.com/de/connect/download/viewer/windows/

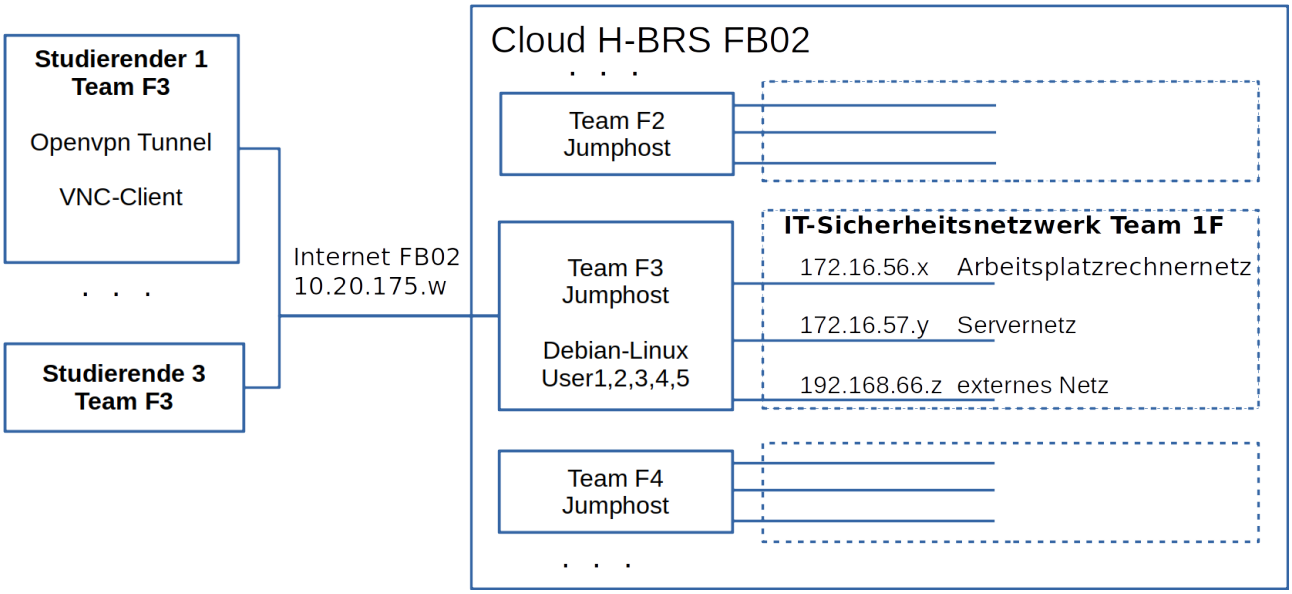
Praktikum zur „IT-Sicherheit“

Beschreibung des Cloud-Zugangs:

Die Aufgaben in diesem Aufgabenblatt werden Sie auf Rechnern in einem Cloud-Umfeld in einer Cloud-Infrastruktur des H-BRS FB02 durchführen.

Dazu benötigen Sie auf Ihrem Rechner einen VNC-Client und einen VPN-Zugang zur Hochschule, wie Sie ihn bereits in anderen Lehrveranstaltungen verwendet haben. Siehe auch:
https://faq.infcs.de/faq/vpn.
Mit dem VNC-Client wählen Sie sich auf den Zugangsrechner (Jumphost) ihres Teams zum IT-Sicherheitsnetzwerk Ihres Teams ein. Die IP-Adresse des Jumphosts Ihres Team finden Sie im LEA-Etherpad hinter Ihrer Team-ID. Arbeiten Sie ausschließlich mit Ihrem Jumphost und dem damit verbundenen Netzwerk.

Auf den Jumphost können Sie sich unter einem der fünf Benutzernamen user1 (PSW: !!user1!), user2 (PWD: !!user2!) ... user5 (PWD: !!user5!) einloggen. Von hieraus können Sie auf Rechner in drei Netzen des IT-Sicherheitsnetzwerks zugreifen (siehe auch nachfolgende Abbildung).



Beschreibung des Experimentierumfeldes:

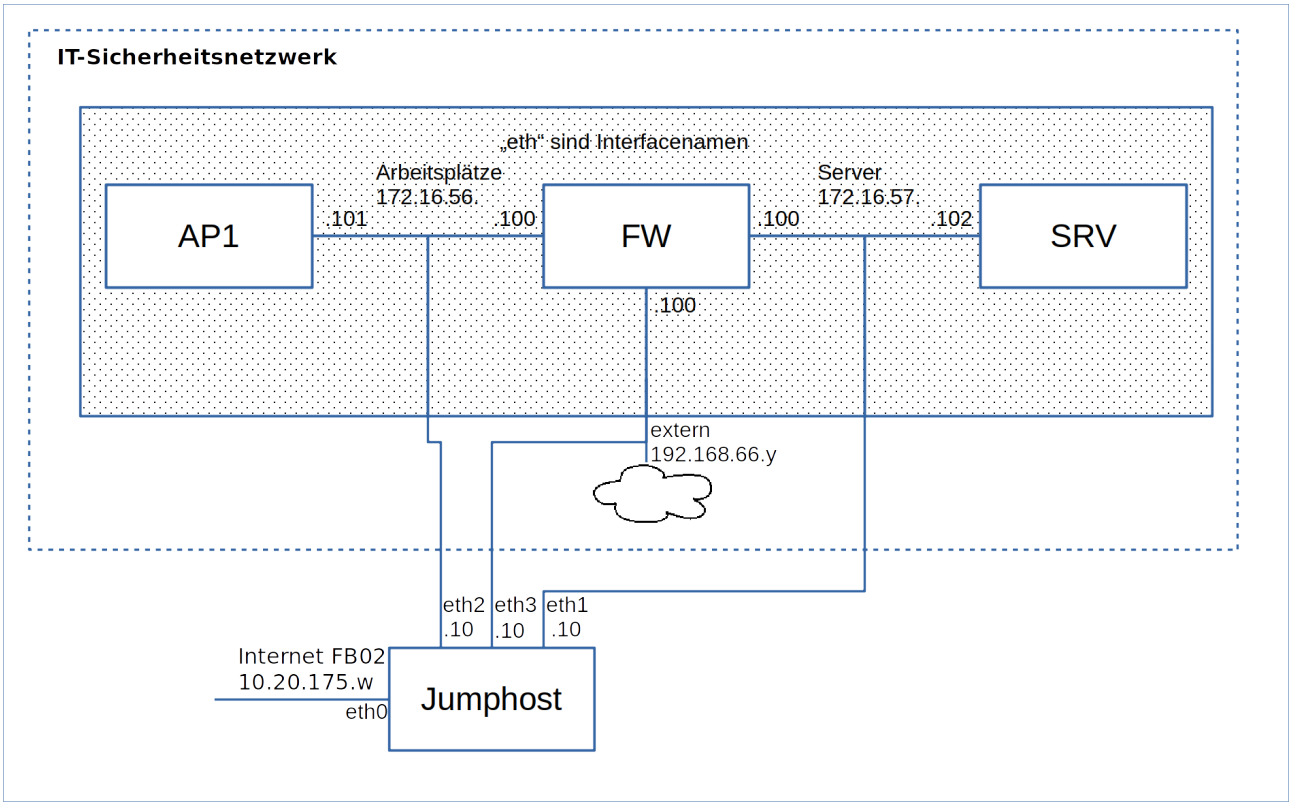
Die Arbeitsumgebung mit drei virtuellen Maschinen (VM) bildet einen Ausschnitt einer Unternehmensnetzinfrastruktur nach. Die Umgebung besteht aus einem Arbeitsplatzrechner (AP1), einem (Web-)Server (SRV) und einem Router bzw. Firewall-Rechner (FW). Die FW verfügt über drei Netzwerkinterfaces und bedient das Arbeitsplatzrechnernetz und das separate Servernetz. Weiterhin besteht über das dritte Interface Verbindung zum Internet. AP1 und SRV verfügen jeweils über ein Netzwerkinterface. Alle IP-Adressinformationen - bis auf die Verbindung zum externen Netz (simuliertes

Praktikum zur „IT-Sicherheit“

allgemeines Internet) sind statisch vergeben.

Die drei Rechner im IT-Sicherheitsnetzwerk Ihres Teams lassen sich über „ssh -X <user>@<ip-addr>“ vom Jumphost erreichen. Das Login in die Maschinen erfolgt im Regelfall als user „root“ mit Passwort „!!root!“. Da hierzu der Zugang über das Arbeitsplatzrechnernetz erfolgt, ist darauf zu achten, dass dieser nicht durch die nftables Konfiguration verwehrt wird. Falls dies doch passiert, kann man über den Firefox-Browser auf dem Jumphost eine extra Konsole erreichen. Diese ermöglicht es, sich interaktiv am betroffenen Rechner anzumelden und z.B. die nftables-Konfiguration zu deaktivieren oder den Rechner im Notfall zu rebooten: „reboot -n“. Der Webzugriff auf die Rechner erfolgt durch folgenden Weblink:

http://10.20.175.155/



Arbeitsplatzrechnernetz: 172.16.56.0/24

Servernetz: 172.16.57.0/24

Externes Netz: 192.168.66.0/24

IP-Adresse AP1 : 172.16.56.101

IP-Adresse FW : 172.16.56.100

: 172.16.57.100

Praktikum zur „IT-Sicherheit“

: 192.168.66.y (Externes Netz)

IP-Adresse SRV : 172.16.57.102

IP-Adresse Jumphost: eth0: 10.20.175.w
eth1: 172.16.57.10
eth2: 172.16.56.10
eth3: 192.168.66.10

Filetransfer von und zum Jumphost

Zum Datenaustausch mit der virtuellen Experimentierumgebung können Sie scp bzw. sftp benutzen. Benutzerinnen und Benutzer von Unix-artigen Betriebssystemen (Linux, MAC OS, Solaris, etc.) haben i.d.R. den benötigten Client schon auf dem System installiert. Setzen Sie Windows ein, können sich z.B. mit PuTTY oder WinSCP aushelfen. In dieser Kurzanleitung wird anhand einiger Anwendungsbeispiele die Benutzung der Werkzeuge gezeigt.

Vorbedingung:

1. Installiertes scp, PuTTY, WinSCP oder ähnliches.
2. Zugang zum Jumphost der jeweiligen Experimentierumgebung.

In diesem Text soll der Jumphost unter der Adresse 10.20.175.94 erreichbar sein. Der Benutzername ist user1. Die gezeigten Kommandos werden auf Ihrem lokalen Rechner ausgeführt.

Anwendungsbeispiele scp

Sie wollen die lokal auf Ihrem Rechner gespeicherte Datei regeln.nft in die Experimentierumgebung in Ihr Heimatverzeichnis kopieren:

```
stella:~> scp regeln.nft user1@10.20.175.94:.
user1@10.20.175.94's password:
regeln.nft
```

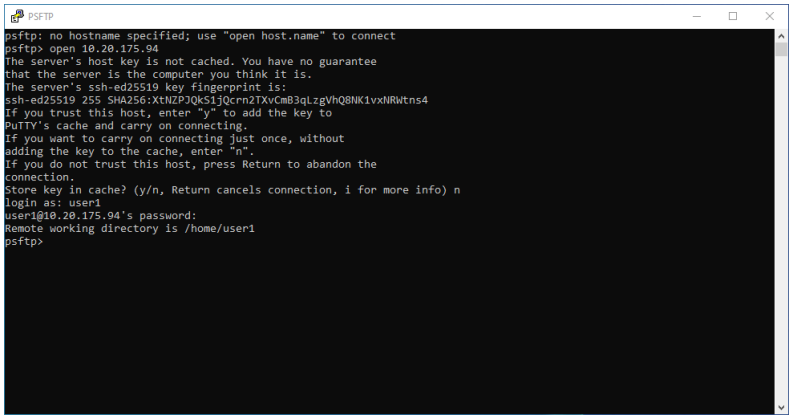
Sie wollen die Datei versuch1.pcap aus dem /tmp-Verzeichnis der Experimentierumgebung auf Ihren lokalen Rechner kopieren:

```
stella:~> scp user1@10.20.175.94:/tmp/versuch1.pcap .
user1@10.20.175.94's password:
versuch1.pcap                                 100%    4     1.2KB/s   00:00
```

Anwendungsbeispiele puTTY

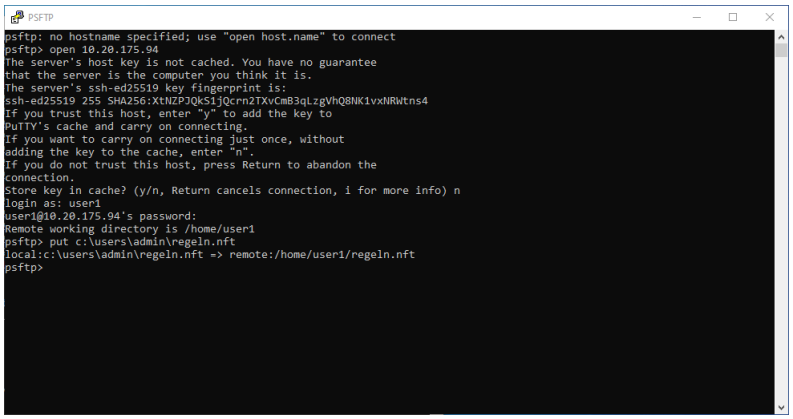
Starten Sie zunächst über das Startmenü die Anwendung PSFTP. Im Anwendungsfenster konfigurieren Sie die Verbindung zum Jumphost Ihrer Experimentierumgebung:

Praktikum zur „IT-Sicherheit“

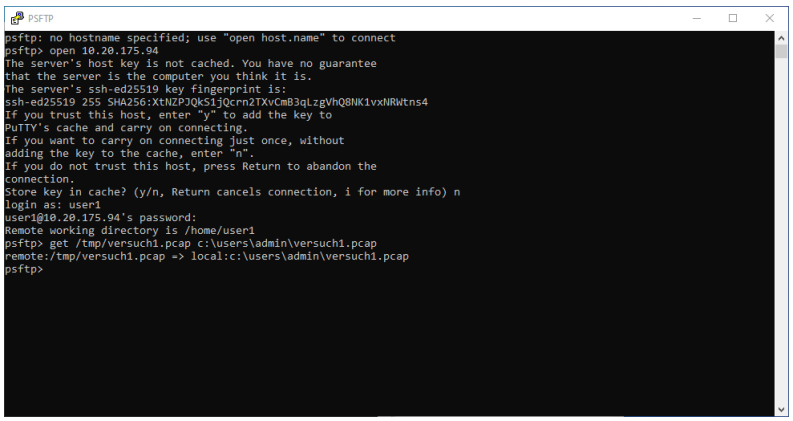


Nach erfolgreicher Anmeldung können Sie die Übertragungskommandos absetzen.

Sie wollen die lokal auf Ihrem Rechner gespeicherte Datei regeln.nft in die Experimentierumgebung in Ihr Heimatverzeichnis kopieren:



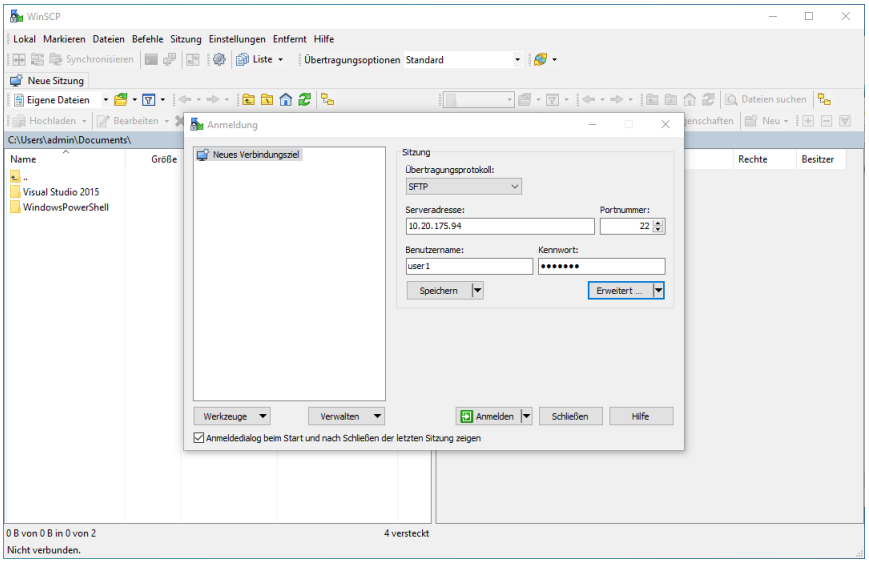
Sie wollen die Datei versuch1.pcap aus dem /tmp-Verzeichnis der Experimentierumgebung auf Ihren lokalen Rechner kopieren:



Praktikum zur „IT-Sicherheit“

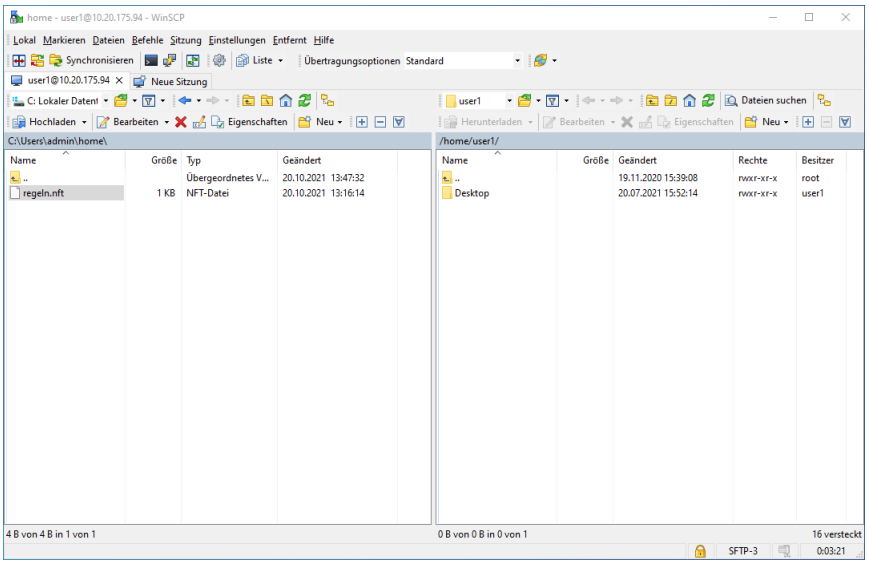
Anwendungsbeispiele WinSCP

Starten Sie zunächst über das Startmenü die Anwendung WinSCP und konfigurieren Sie die Verbindung zum Jumphost Ihrer Experimentierumgebung:



Bestätigen Sie die Eingaben mit der Schaltfläche Anmelden. Nach erfolgreicher Anmeldung können Sie im Anwendungsfenster die Dateiübertragungen durchführen.

Das Anwendungsfenster ist zweigeteilt: auf der linken Seite finden Sie Ihr lokales Dateisystem, auf der rechten Seite das Dateisystem des Jumphosts. Sie können z.B. über drag and drop Dateien austauschen:



Sichern von Wireshark-Ergebnissen

Sichern Sie die Aufzeichnungen aus Wireshark zu jeder Teilaufgabe in einer

Praktikum zur „IT-Sicherheit“

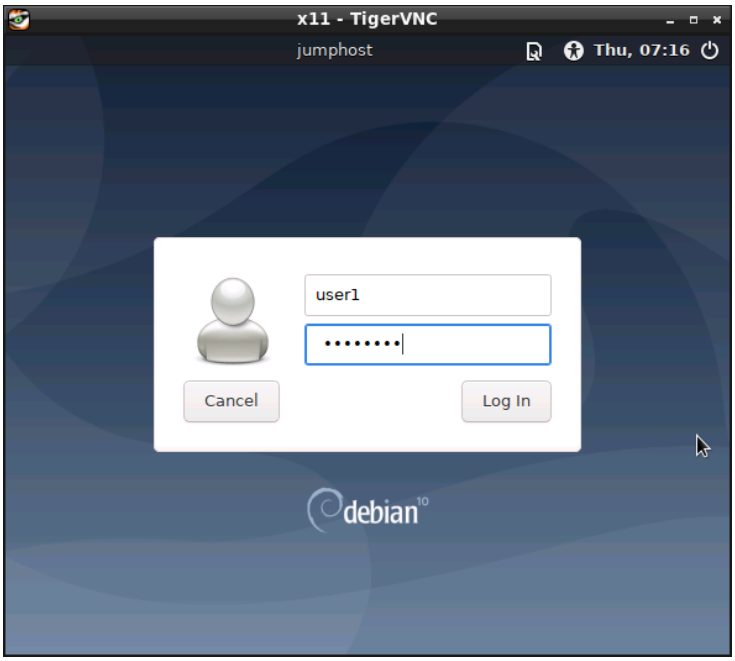
„.pcapng“ Datei mit Aufgabenteil als Name und übertragen Sie diese Dateien zu Ihrem persönlichen Rechner (nicht Cloud). Damit können Sie die Ergebnisse auch lokal analysieren. Beachten Sie, dass manche Mitschnitte von wireshark in dieser Netzwerkumgebung in kurzer Zeit sehr groß werden können: Achten Sie deshalb auch auf die Größe der Dateien, verkürzen Sie ggf. die Zeitdauer des Mitschnitts. **Halten Sie diese Daten zur Abnahme bereit.**

P.1. Wireshark Einstieg (Gruppenaufgabe)

Wireshark ist ein Programm zur passiven Analyse der Netzwerkkommunikation, bzw. ein „Sniffer“-Tool. Wireshark ist auf dem Jumphost und auf AP1 bereits vorinstalliert.

1. Wählen Sie sich mit ihrem VNC-Client auf den Jumphost Ihres Teams ein (siehe Etherpad bei Ihrem Team)

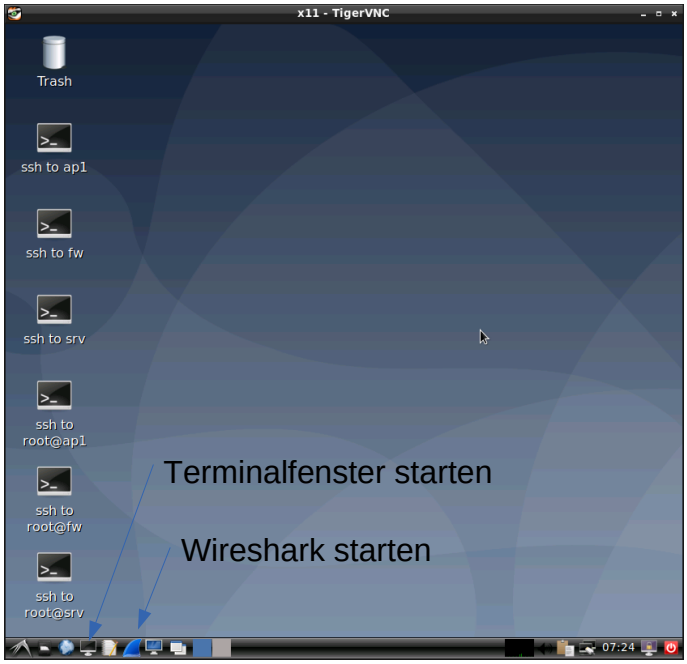
   z.B. `vncviewer 10.20.175.125`



   Hier wurde als Beispiel user1 gewählt. Wählen Sie unterschiedliche Benutzer in Ihrem Team.

   Es erscheint die Linux-Oberfläche des jeweiligen users auf dem Jumphost.

Praktikum zur „IT-Sicherheit“



2. Öffnen sie ein Terminalfenster und lassen Sie sich die Interfaces mit dem Befehl ip -br a anzeigen. Vergleichen Sie die Ausgabe mit den Abbildungen des Sicherheitsnetzwerkes am Anfang dieses Aufgabenblattes.
3. Starten Sie Wireshark auf dem Jumphost und zeichnen Sie ca. 30 Sekunden den Datenverkehr auf allen Interfaces (any) auf. Welche Protokolle sehen Sie? Beenden Sie den Mitschnitt. Speichern Sie den Mitschnitt.
4. In dieser Aufgabe sollen Sie ein „ping“ zu einem Rechner (ap1, fw, srv) im IT-Sicherheitsnetzwerk Ihrer Gruppe aufzeichnen. Starten Sie einen neuen Mitschnitt (unter „Captures Options“) und wählen Sie dabei das passende Netzwerkinterface auf dem Jumphost zur Aufzeichnung Ihres ping aus. Welches Interface haben Sie gewählt? Was sind die beteiligten IP- und MAC-Adressen, die Sie in der Aufzeichnung sehen? Beenden Sie den Mitschnitt. Speichern Sie den Mitschnitt.
   Hinweis: Beim Neustart eines Captures kann es notwendig sein, die Zeile des Displayfilters von Wireshark einmal ohne Inhalt mit Enter anzuklicken, damit die neu aufgezeichneten Pakete angezeigt werden.
5. Testen Sie, dass Sie einen gespeicherten Mitschnitt wieder in wireshark importieren können.

P2. Wireshark Filter (Gruppenaufgabe)

Wireshark beinhaltet zwei Filtermethoden: Display-Filter (unter Menü Analyze) und Capture-Filter (unter Menü Capture). Einführungen dazu siehe Hinweislinks am Anfang des Aufgabenblattes.

Wählen Sie bei den folgenden Aufzeichnungen das „any“-Interface.

Praktikum zur „IT-Sicherheit“

1. **Test des Display-Filters**:
    1. Starten Sie einen neuen Mitschnitt (unter „Captures Options“) mit Interfaces „any“. Führen Sie jetzt erneut ein „ping“ zu einem Rechner (ap1, fw, srv) im IT-Sicherheitsnetzwerk durch. Definieren Sie jetzt Filter, die die Ping-Pakete anzeigen und möglichst keine anderen. Welche Filterregeln führen zum Ziel? **Dokumentieren Sie Ihre Filterregeln.**
    2. Starten Sie einen neuen Wireshark-Mitschnitt. Öffnen Sie den Browser und geben Sie die Adresse „www.knoppix.de“ ein. Beenden Sie den Mitschnitt. Selektieren Sie mit dem Displayfilter alle Datenpakete, die das Protokoll http verwenden. Speichern Sie den Mitschnitt.

2. **Test des Capture-Filters**:
    1. Konfigurieren Sie den Wireshark-Mitschnitt bei den Capture Interface-Options so, dass Sie nur die Pakete mit dem http-Protokoll aufzeichnen. Geben Sie hierfür eine Capture-Filterregel an. Starten Sie diesen neuen Wireshark-Mitschnitt. Öffnen Sie den Browser und geben Sie die Adresse „www.knoppix.de“ ein. Beenden Sie den Mitschnitt. Speichern Sie den Mitschnitt. **Dokumentieren Sie Ihre Filterregeln.**

3. Wann wählen Sie welche Filtermethode in der Praxis? Dokumentieren Sie Vor- und Nachteile beider Verfahren.

4. Suchen Sie mit einer Filtermethode ihrer Wahl in Ihren Mitschnitten mit www.knoppix.de nach dem String „Rescue-System“ und überzeugen Sie sich, dass Sie den Inhalt der Webseite in Wireshark sehen.

    Hinweise: Nutzen Sie Display-Filter und die Funktionalität „Follow HTTP Stream“ von Wireshark. Um alle Teile der Webseite erneut zu erhalten kann ein Neustart des Browsers oder Löschen des Caches im Browser erforderlich sein.

P.3. Passwort Sniffing mit Wireshark (Gruppenaufgabe)

Starten Sie eine neue Wireshark Aufzeichnung für den srv-Rechner. Starten Sie den Browser auf dem Jumphost und geben Sie die Adresse „srv.itsecnet.de“ ein. Geben sie einen beliebigen User und ein beliebiges Passwort ein. Finden Sie den eingegebenen User und das Passwort im Wiresharkmitschnitt und dokumentieren Sie dies mit einem Screenshot von Wireshark. Speichern Sie den Mitschnitt.

Können User und Passwort auch von einem Gruppenmitglied auf dem Jumphost mit Wireshark gefunden werden, das sich nicht bei „srv.itsecnet.de“ angemeldet hat?

P.4. Web-Datenverkehr analysieren mit Wireshark (Gruppenaufgabe)

Da Browser zunehmend die Nutzer vor unverschlüsselten http-Webseiten warnen, hat ein Wechsel zum https-Protokoll bei den meisten Webserverbetreibern bereits stattgefunden.

In dieser Aufgabe soll der Datenverkehr der Webseite „www.heise.de“ analysiert werden.

1. Starten Sie einen neuen Wireshark-Mitschnitt ohne Verwendung von speziellen Capture-Filtern. Geben Sie in dem Browser die Adresse „www.heise.de“ ein. Beenden Sie kurz nach dem Aufbau der Webseite den Mitschnitt. Speichern Sie den Mitschnitt.
2. Analysieren Sie mit Wireshark, von wie vielen IP-Adressen Daten nach dem Aufruf der Webseite „www.heise.de“ geladen worden sind. Nutzen Sie dazu die Option Endpoints unter dem Menü Statistics in Wireshark.
3. Analysieren Sie, mit welchen Endpunkten eine **http-**Kommunikation stattgefunden hat. Analysieren Sie für jeden gefundenen Endpunkt mit http-Kommunikation: Welche Aufgabe wurde vermutlich mit dieser http-Kommunikation verfolgt? Arbeiten Sie in dieser Aufgabe in der Gruppe parallel, d.h. teilen Sie die Analyse der Endpunkte innerhalb Ihrer Gruppe auf und sammeln Sie die Ergebnisse.
   Hinweise:
   Sie können die Ports nach Nummern sortieren.
   Lassen Sie sich mit „Name Resolution“ (Links unten) die Adressauflösungen der gefundenen Endpunkte mit Wireshark anzeigen.
   Für jede ausgewählte Zeile können sie mit „rechter Maustaste“ einen Displayfilter aktivieren.

   Nutzen Sie Displayfilter und die Funktionalität „Follow TCP Stream“ bzw „Follow HTTP Stream“von Wireshark.
4. Wählen Sie einen Endpunkt mit **https-**Kommunikation aus und analysieren Sie den Beginn der Kommunikation mit diesem Endpunkt. Welche Nachrichten werden ausgetauscht?

P.5. Mitschnitte lokal speichern

Übertragen Sie alle Ihre Mitschnitte auf einen lokalen Rechner und speichern Sie sie auch dort.

Praktikum zur „IT-Sicherheit“

Vorbereitung für den Abnahmetermin

1. Präsentation in BBB-Räumen üben.
    - Siehe LEA (BBB-Räume zur Team-Kollaboration).
    - Funktion der Webcam prüfen
    - Funktion des Mikrofons prüfen
    - Mit einem Teammitglied eine Präsentation üben.
2. Studierendenausweis und Lichtbildausweis zur Kontrolle bereit halten.
3. VNC-Client mit der Internetadresse des Jumphosts (steht im LEA-Teameinteilung Etherpad) vorher starten und als ein User einloggen.
4. Ihre Ergebnisse der Aufgaben für eine Anzeige in der Bildschirmfreigabe vorbereiten.

Was sie für das Fachgespräch im Praktikumstermin für eine erfolgreiche Abnahme können müssen

1. Die Vernetzung des IT-Netzwerks erklären.
2. Sich in die Rechner AP1, FW und SRV einloggen und die Rechner bedienen.
3. Einfache Fragen zur Aufgabe des Tools wireshark beantworten können.
4. Einfache Filterstrings erklären und erstellen können.
5. Aufgaben dieses Praktikumsaufgabenblatts mit Wireshark live vorführen.
6. Aufgezeichnete Wiresharkmitschnitte dieses Praktikumsaufgabenblatts mit Wireshark anzeigen und filtern.
7. Vorbereitete Screenshots, Filterregeln und Analyseergebnisse in der Freigabe anzeigen und erläutern können.