


Übungsprotokoll

ITSI – Informationstechnologie Sicherheit

	Übungsdatum: 24.02.2021	Klasse: 2AHIT	Name: Felix Schneider
	Abgabedatum: 24.02.2021	Gruppe: ITS12	Note:
Leitung: Jürgen HAUPTMANN	Mitübende: -		
Übungsbezeichnung: Apache2 Passwort lesen + nicht lesen			

Inhaltsverzeichnis:

1	Aufgabenstellung.....	2
2	Abstract (English).....	2
3	Theoretische Grundlagen	2
4	Übungsdurchführung.....	3
5	Ergebnisse.....	5
6	Code	6
7	Kommentar	6

1 Aufgabenstellung

Apache2 mit HTTP Auth am Router installieren nach folgender Anleitung:

<https://blog.net-solve.at/post/12>

Wenn alles läuft, Wireshark am Router starten und versuchen das eingestellte Passwort herauszufinden.

Apache2 mit HTTPS Auth am Router installieren nach folgender Anleitung:

<https://blog.net-solve.at/post/13>

Wenn alles läuft, Wireshark am Router starten und versuchen das eingestellte Passwort herauszufinden.

2 Abstract (English)

Install Apache2 with HTTP Auth on the router according to the following instructions:

<https://blog.net-solve.at/post/12>

If everything works, start Wireshark on the router and try to find out the set password.

3 Theoretische Grundlagen

Theoretische Grundlagen, die zum Verständnis erforderlich sind.

Z. B. bei DHCP: Sinn und Zweck, Einsatzmöglichkeiten, Verweis auf Spezifikationen, ...

4 Übungsdurchführung

4.1 Apache2 installieren

Als allererstes muss Apache2 auf dem Router-Rechner installiert werden, dies funktioniert mit dem Befehl:

```
apt install apache2
```

4.2 Authentifizierungspaket installieren

```
sudo apt install apache2-utils
```

4.3 neuen HTTP-Benutzer anlegen

```
htpasswd -c /etc/apache2/.htpasswd user1234
```

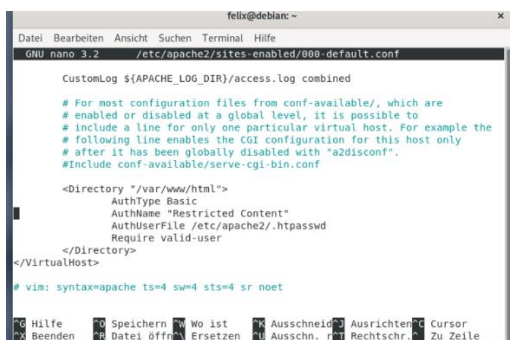
```
root@debian:~# htpasswd /etc/apache2/.htpasswd user1234
htpasswd: cannot modify file /etc/apache2/.htpasswd; use '-c' to create it
root@debian:~# htpasswd -c /etc/apache2/.htpasswd user1234
New password:
Re-type new password:
Adding password for user user1234
root@debian:~#
```

4.4 Apache bearbeiten

Die Datei /etc/apache2/sites-enabled/000-default.conf muss noch konfiguriert werden, sodass sie so aussieht:

```
<VirtualHost *:80>
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    <Directory "/var/www/html">
        AuthType Basic
        AuthName "Restricted Content"
        AuthUserFile /etc/apache2/.htpasswd
        Require valid-user
    </Directory>
</VirtualHost>
```



4.5 Apache-Server neu starten

#service apache2 restart

```
root@debian:~# service apache2 restart
Failed to restart apache.service: Unit apache.service not found.
root@debian:~# apache restart
-bash: apache: Kommando nicht gefunden.
root@debian:~# service apache2 restart
root@debian:~# nano /etc/apache2/sites-enabled/000-default.conf
```

4.6 Wireshark vorbereiten

Wireshark öffnen und mit Loopback lo starten.

4.7 auf localhost gehen

Firefox öffnen, localhost in die URL eingeben, Benutzername und Passwort eintippen.

4.8 In Wireshark Passwort finden

In Wireshark im Anzeigefilter http eingeben, ein GET-Paket auswählen und anschließend in dieser Datei nach Authentification suchen. Auf den Pfeil davor klicken und Benutzername und Passwort stehen.

```
Authorization: Basic dXNlcjEyMzQ6cmFuZG9t\r\n
Credentials: user1234:random
```

The screenshot shows the Wireshark interface with the following details:

- Filter:** http
- Packet List:** Shows a list of captured packets. Packet 39 is selected, which is an HTTP GET request to localhost.
- Packet Details:**
 - Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)
 - Internet Protocol Version 6, Src: ::1, Dst: ::1
 - Transmission Control Protocol, Src Port: 41958, Dst Port: 80, Seq: 1, Ack: 1, Len: 490
 - Hypertext Transfer Protocol
 - GET / HTTP/1.1\r\n
 - Host: localhost\r\n
 - User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0\r\n
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
 - Accept-Language: de,en-US;q=0.7,en;q=0.3\r\n
 - Accept-Encoding: gzip, deflate\r\n
 - Authorization: Basic dXNlcjEyMzQ6cmFuZG9t\r\n
 - Credentials: user1234:random
 - Connection: keep-alive\r\n
 - Upgrade-Insecure-Requests: 1\r\n
 - If-Modified-Since: Wed, 10 Feb 2021 09:17:09 GMT\r\n
 - If-None-Match: "29cd-5baf7de14a414-gzip"\r\n
 - Cache-Control: max-age=0\r\n
 - \r\n
 - [Full request URI: http://localhost/]
 - [HTTP request 1/2]
- Packet Bytes:** Shows the raw data of the request, including the Authorization header and the body.

4.9 HTTPS

<https://blog.net-solve.at/post/13>

4.10 Screenshots

```

root@debian:~# openssl genrsa -out www.server1.com.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....
...+++++
.....+++++
e is 65537 (0x010001)
root@debian:~#

felix@debian: ~
Datei Bearbeiten Ansicht Suchen Terminal Hilfe
GNU nano 3.2 /etc/hosts
127.0.0.1 www.server1.com
127.0.1.1 debian

# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

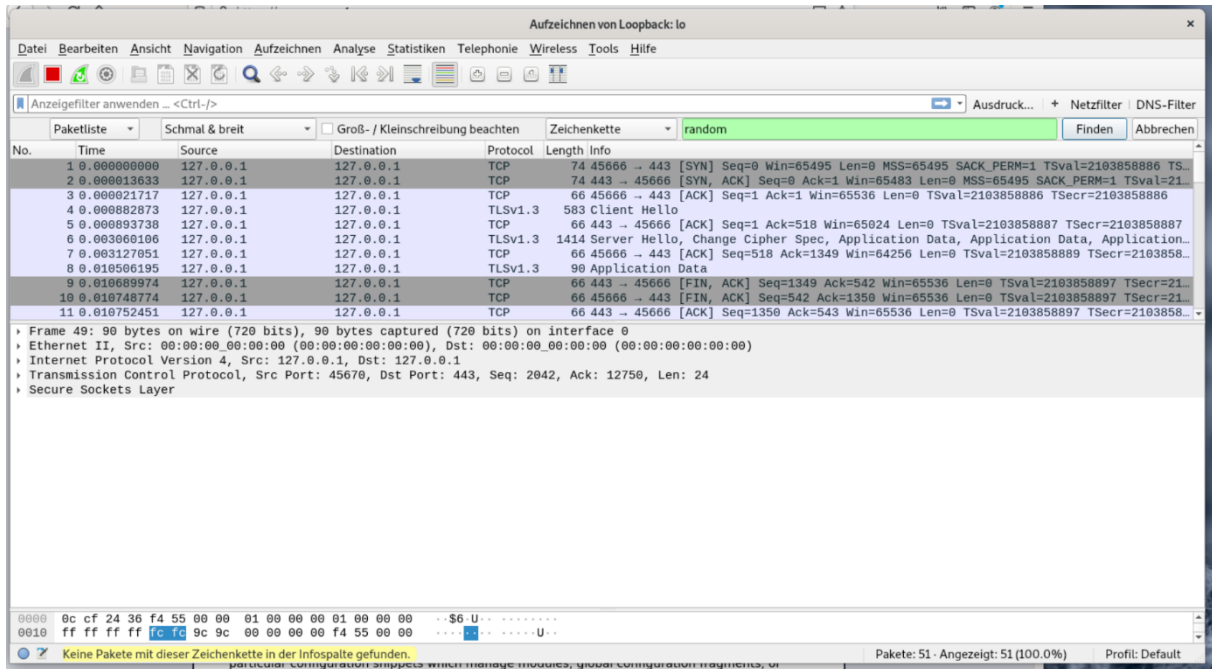
root@debian:~# openssl req -new -key www.server1.com.key -out www.server1.com.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:au
State or Province Name (full name) [Some-State]:Austria
Locality Name (eg, city) []:Krems
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:random
An optional company name []:
root@debian:~#

root@debian:~# openssl x509 -req -days 365 -in www.server1.com.csr -signkey www
.server1.com.key -out www.server1.com.crt
x509: Unrecognized flag signkey
x509: Use -help for summary.
root@debian:~# openssl x509 -req -days 365 -in www.server1.com.csr -signkey www.
server1.com.key -out www.server1.com.crt
Signature ok
subject=C = au, ST = Austria, L = Krems, O = Internet Widgits Pty Ltd
Getting Private key
root@debian:~# ls
-q www.server1.com.crt www.server1.com.csr www.server1.com.key
root@debian:~# ls -al

```

```
root@debian:~# a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
    systemctl restart apache2
root@debian:~#
```



5 Ergebnisse

In Wireshark findet man Benutzername und Passwort in dem Format:

benutzername:passwort

6 Code

Optionales Kapitel für Source Codes von Programmen, Skripten o. ä.

7 Kommentar

http ist unsicherer als HTTPS bzw. http ist nicht verschlüsselt.