

Security Engineering

1. Übung

Vorbemerkung:

- Sie können Ihr eigenes Gerät mitbringen (Notebook/Laptop).
- Beachten Sie die Hinweise aus der Vorlesung (Linux/Terminal).
- Labor IT-Sicherheit
 - hat FreeBSD-Maschinen isl-l-01, ..., isl-l-08 installiert
 - nutzt STL-User-Accounts
- Einloggen von Ihrem Laptop aus via `ssh` zu `stl-s-stud` und weiter zu einem der `isl-` Rechner:

```
ssh -l username stl-s-stud.htwsaar.de
...
ssh isl-l-01.htwsaar.de
```

(den detaillierten Ablauf finden Sie auf der letzten Seite).

https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html

Aufgabe 1 (C Programm)

Das Kommando `date` gibt das aktuelle Datum mit Uhrzeit aus.

Schreiben Sie ein C-Programm, das den Zeitpunkt in der folgenden Form ausgibt:

Thu Apr 21 14:13:38 2022

a) mit Hilfe von `time()`, gefolgt von `ctime()`

b) mit Hilfe von `time()`, gefolgt von `localtime()` und `strftime()`

Falls Sie Informationen zu den C-Funktionen benötigen, hilft Ihnen das `man`-Kommando:

```
man 3 time
```

```
man 3 strftime
```

Aufgabe 2 (Hashfunktionen zur Prüfen der Integrität von Dateien)

Es gibt innerhalb der Systemkommandos auf Linux und FreeBSD-Systemen Hashfunktionen: in der Reihenfolge ihrer Wichtigkeit

sha256, sha1, sha384, md5

Wenden Sie diese Hashfunktionen an, um festzustellen, dass die Datei `/etc/services` nicht verändert wurde:

```
SHA256 (/etc/services) = ccda4683295b09834e17b1cce0c3c1945ec197...
SHA1 (/etc/services) = c42cb3105eac07d79fecb69976c7204818ee5415
SHA384 (/etc/services) = ab9487cfced4a262384de746430fdbfc0f8c97...
MD5 (/etc/services) = 89ad32116c62bee2a1eb3798d2583c96
```

Kopieren Sie die Datei `/etc/services` in Ihr Homeverzeichnis und verändern Sie einen Eintrag. Stellen Sie fest, dass dadurch der Hashwert verändert wird.

Geben Sie den Hashwert auch mittels `openssl` aus.

```
openssl dgst -sha1 ...
```

OpenSSL stellt noch weitere sichere Hashfunktionen zur Verfügung, probieren Sie insbesondere SHA512, whirlpool, RIPEMD160.

Aufgabe 3 (Kryptoschlüssel erzeugen)

Erzeugen Sie sich einen RSA-Kryptoschlüssel mit 2048 Bit.

```
$ ssh-keygen -t rsa -b 2048
```

```
Generating public/private rsa key pair.
```

```
Enter file in which to save the key (/export/home_pm/dweber/.ssh/id_rsa):
```

```
Enter passphrase (empty for no passphrase):
```

Enter same passphrase again:

Your identification has been saved in /export/home_pm/dweber/.ssh/id_rsa.
Your public key has been saved in /export/home_pm/dweber/.ssh/id_rsa.pub.

The key fingerprint is:

3d:96:a1:ab:cf:9a:ff:d6:f2:de:e6:10:d5:60:e5:d4 dweber@stl-s-studwork

Fügen Sie den Key aus id_rsa.pub zu der Datei

`${HOME}/.ssh/authorized_keys`

eines Zielrechners hinzu.

Jetzt können Sie sich ohne Passworteingabe auf diesen Zielrechner einloggen. Wenn Sie sich ohne Passworteingabe vom `stl-s-stud.htwsaar.de` zum `isl-1-01.htwsaar.de` verbinden wollen, müssen Sie den Key auf dem `stl-s-stud` erzeugen und in der `authorized_keys` eines `isl`-Rechners eintragen.

Falls Sie nur Windows-Systeme im Zugriff haben sollten, können Sie mit dem PuTTY-Client und der Anleitung

<https://www.howtoforge.de/anleitung/key-basierte-ssh-logins-mit-putty/>

einen Schlüssel für Ihren Windows-Client erzeugen.

Hinweis: Vorgang zum Einloggen in das ISL-Netz

von zu Hause oder vom HTW-WLAN aus:

```
$ ssh -l stl-login-name stl-s-stud.htwsaar.de
```

```
The authenticity of host 'stl-s-stud.htwsaar.de (134.96.216.212)' can't be established.
```

```
RSA key fingerprint is 00:c3:5b:21:6a:c0:ad:3f:03:37:1c:e0:88:bf:82:7b.
```

```
No matching host key fingerprint found in DNS.
```

```
Are you sure you want to continue connecting (yes/no)? yes
```

```
Warning: Permanently added 'stl-s-stud.htwsaar.de' (RSA) to the list of known hosts.
```

```
Password: *****
```

```
Last login: Fri Apr 17 11:03:02 2015 from pd9e08fd4.dip0.
```

```
$ ssh isl-l-01
```

```
The authenticity of host 'isl-l-01 (134.96.216.81)' can't be established.
```

```
RSA key fingerprint is 04:5d:22:aa:dc:d6:67:27:8e:a7:db:10:2e:03:7e:5e.
```

```
Are you sure you want to continue connecting (yes/no)? yes
```

```
Warning: Permanently added 'isl-l-01,134.96.216.81' (RSA) to the list of known hosts.
```

```
Password: *****
```

```
Last login: Tue Apr 18 11:43:37 2023 from :0 FreeBSD 13.2-BETA1
```

```
#0 releng/13.2-n254465-da0a75e1cf07: Sat Feb 11 00:02:19 UTC 2023
```

```
root@releng3.nyi.freebsd.org:/usr/obj/usr/src/amd64.amd64/sys/GENERIC
```

```
stl-login-name@isl-l-01(1)$
```