



SVS | Exercise 2

Task 1 (optional)

Falls Sie kein Linux auf Ihrem System installiert haben, richten Sie eine virtuelle Maschine mit dem Image unter <https://mytuc.org/cntn> ein. In dem Image sind alle für die Übung erforderlichen Werkzeuge vorinstalliert (Wireshark, PHP, Openssl, Apache Webserver).

If you do not have any Linux system on your PC, install and get acquainted with the following virtual machine: <https://mytuc.org/cntn>. The image has pre-installed tools required for the next tutorials (Wireshark, PHP, Openssl, Apache Webserver).

Task 2

Betrachten Sie das Programm *over.c* (siehe OPAL). Das Programm akzeptiert Verbindungen an einem gegebenen Port und fragt die Gegenseite nach einem Passwort. Falls das Passwort „lula“ eingegeben wird, dann wird ein Geheimnis angezeigt, ansonsten eine Fehlermeldung.

- Überlegen Sie sich, was man eingeben könnte, um sich das Geheimnis trotz des fehlenden Passwortes anzeigen zu lassen!
- Kompilieren Sie das Programm (`cc over.c -o over`), starten Sie es an einem freien Port (`./over 9000`) und verbinden Sie sich mit dem Prozess mittels telnet (`telnet localhost 9000`). Geben Sie Ihre Zeichenkette ein¹.

Consider the program *over.c* (cf. OPAL). The program accepts incoming connections on a given port and asks the communication partner for a password. If the entered password is „lula“, then a secret is shown, otherwise an error message.

- Think about, what can be entered to show the secret without knowing the password.
- Compile the Program (`cc over.c -o over`), start it on some free port (`./over 9000`) and connect to it using telnet (`telnet localhost 9000`). Enter your string¹.

Task 3

Machen Sie sich mit dem Werkzeug Wireshark² vertraut (in dem Image aus der Aufgabe 1 enthalten; muss mit *root*-Rechten gestartet werden). Rufen Sie die Seite <http://vsr-wss1.informatik.tu-chemnitz.de> im Browser auf und nehmen Sie die dabei übertragenen Daten auf.

- Wie sind die HTTP-Nachrichten aufgebaut?
- Welche HTTP-Header werden vom Browser mitgeschickt und welche Bedeutung haben diese?

Get acquainted with the tool Wireshark² (available on the image from task 1; should be started with root rights). Request the resource <http://vsr-wss1.informatik.tu-chemnitz.de> using a browser and record the transferred data using Wireshark.

- What is the structure of HTTP messages?
- Which HTTP Header are sent and what is their meaning?

¹ Der Angriff kann auf manchen Betriebssystemen und Compilern nicht funktionieren. Probieren Sie die virtuelle Maschine aus der Aufgabe 1 oder `-fno-stack-protector` beim Kompilieren. / The attack can fail on some of operating systems and compilers. Try out the virtual machine from the task 1 or `-fno-stack-protector` at compiling.

² <http://www.wireshark.org/>

Task 4

Das Programm *zugriff* dient dem Zugriff auf <http://vsr-wss1.informatik.tu-chemnitz.de/zugriff/feier.xhtml>, der ansonsten wegen der fehlenden Kenntnisse des Nutzernamens nebst Passwort nicht möglich ist.

- Lesen Sie im RFC2617³ nach, wie die HTTP Basic Authentication abläuft!
- Ermitteln Sie Nutzerkennzeichen und Passwort, die zum Zugriff auf diese Seite notwendig sind! Finden Sie mit Hilfe des Programms *zugriff* heraus, wo die völlig geheime Feier stattfindet!

The program *zugriff* can be used to access <http://vsr-wss1.informatik.tu-chemnitz.de/zugriff/feier.xhtml>, which is otherwise not possible due to missing username and password.

- Find out in RFC2617, how HTTP Basic Authentication works.
- Find out username and password required to access the above resource. Find out where the completely secret party takes place!

³ <http://tools.ietf.org/html/rfc2617>