Telematics

Winter Semester 2010/11

Number:	14. Assignment
Issued:	03.02.11
Tutorial:	10.02.11
Lecturer:	Prof. Dr. Güneş, Dipl.-Inf. Blywis
Contact:	{guenes, blywis}@inf.fu-berlin.de

Exercise 1, SSH Tunneling:

As you probably know, SSH can be used to create (secure) tunnels. Follow the steps to access the Telematics assignments over an SSH tunnel.

1. You need a console SSH client or some alternative, e.g., PuTTY: `http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html`
2. Setup the SSH tunnel with some random local port and port 80 as endpoints between your host and some faculty computer, e.g., xian:
   `ssh -L LOCAL_PORT:cst.mi.fu-berlin.de:80 USER@xian.imp.fu-berlin.de`
3. Add the following mapping in the hosts file in you operating system:
   `127.0.0.1 cst.mi.fu-berlin.de`
   The location is operating system specific. Examples:
   - Linux, BSD: /etc/hosts
   - Windows: `%SystemRoot%\system32\drivers\etc\`
4. Open the following URL in a web browser:
   `http://cst.mi.fu-berlin.de:LOCAL_PORT`
5. Download one of the Telematics assignments
6. Use Wireshark or any alternative tool to capture the data traffic between the two hosts

Explain why step 3 is required and what happens when it is omitted.

Exercise 2, Traffic Shaping:

Explain the token and leaky bucket schemes and how they are applied in computer networks.

Exercise 3, Firewalls:

What are firewalls and on which layer(-s) of the ISO/OSI reference model do they operate?

Exercise 4, Secure Network Topology:

Connect a LAN to the Internet. To enable world-wide access to services that your servers provide, addresses from 137.226.12.32/29 are available. The internal/private network uses addresses from 192.168.0.0/16.
The following services are provided by hosts in the network for users from the LAN or word-wide network.

Service	LAN	world-wide
WWW server	×	×
SMTP server	×	×
SMTP and POP3 server	×	
DNS server 1	×	×
DNS server 2	×	
DHCP server	×	
Printer with network connection	×	
Management server with administration tools	×	
Multiple workstations	×	

In addition there are two firewalls available: one stateless and one stateful.

1. Create a network topology which considers all requirements and assign IP addresses to all hosts.
2. Define rule sets for both firewalls:
   - Rules are evaluated one after another according to their order. The first matching rule is applied by performing the assigned action; all following rules are ignored.
   - Rules consist of two parts: a condition and an action. Use the following notation as rule format:

     `<Protocol, Src IP, Src Port, Dest. IP, Dest. Port, [State,] Action>`

     – State: Used only in the stateful firewall. Defines the state of a TCP connection. The value `ESTAB` represents an established TCP connection (packets with a set `ACK` flag). `SYN` matches to segments with set SYN flag.
     – Action: May have the values `ALLOW` and `DENY`.
     – The wildcard "`*`" matches any value
   - Example:

     `<TCP, 123.45.0.0/16, *, 198.182.196.56, 80, SYN, ALLOW>`

     TCP segments with set SYN flag from any host in 123.45.0.0/16 and destined to host 198.182.196.56 on port 80 are allowed to pass the firewall.

Exercise 5, Peer-To-Peer Networking:

1. Discuss the peer-to-peer (P2P) networking principle
2. Name and explain properties to classify P2P networks

Exercise 6, Movie Time:

- Watch the movie *Warriors of the Net*: download
- Look for "inaccuracies" and discuss the content / representation of computer networks in the tutorial session.

Exercise 7, Up and Down:

How often is the protocol stack traversed when a host is connected to a network and the user tries to view a website in the browser?