

# Betriebssystem UNIX - Systemadministration und Sicherheit

## 6.Praktikum (22.1.2014)

### 1. Deaktivieren Sie den Firewall Ihrer Maschine

- Deaktivieren Sie den Firewall Ihrer Maschine.
- Welche Ports sind lokal offen?
- Welche Ports sind von anderen Maschinen aus sichtbar?

### 2. Aktivieren Sie den Firewall Ihrer Maschine

- Aktivieren Sie den Firewall Ihrer Maschine
- Lassen Sie nur interne Verbindungen zu. Verboten Sie alle externen Verbindungen (in und out)
- Welche Ports sind lokal offen
- Welche Ports sind von anderen Maschinen aus sichtbar?
- Lassen Sie ausgehende externe Verbindungen zu.
- Welche Ports sind von anderen Maschinen aus sichtbar?
- Lassen Sie zusätzlich alle eingehenden SSH-Verbindungen zu.
- Welche Ports sind von anderen Maschinen aus sichtbar?
- Lassen Sie die eingehenden SSH-Verbindungen nur von zwei Rechnern Ihrer Wahl aus zu
- Welche Ports sind von den ausgewählten Rechnern aus sichtbar?
- Welche Ports sind von allen anderen Rechnern aus sichtbar?

### 3. NFS und Firewall

- Richten Sie auf Ihrem Rechner einen NFS-Server ein und exportieren das Directory /home.
- Versuchen Sie das exportierte Directory /home von einem anderen Rechner aus zu mounten (z.B. mount treptow:/home /mnt).
- Modifizieren Sie den Firewall so, dass das Mounten nur von dem anderen Rechner aus funktioniert.
- Welche Ports sind von dem anderen Rechner aus sichtbar?
- Welche Ports sind von allen anderen Rechnern aus sichtbar?

Hilfestellung:

Anzeigen lokaler offener Ports: **netstat**

**netstat -a -t** - offene TCP-Ports

**netstat -a -u** - offene UDP-Ports

Anzeigen offener Ports auf entfernten Rechnern: **nmap** (zypper install nmap)

**nmap -sT treptow** - sichtbare TCP-Ports

**nmap -sU treptow** - sichtbare UDP-Ports

Achtung!!! nmap nur für Zielrechner des Praktikumpools benutzen!!!!