„Linux – network security”

Course description:

Linux training – network security is addressed to Linux administrators and network administrators who want to learn about network security techniques in Linux. The participants of Linux training – network security should have basic knowledge of Linux and networks in this system.

Training program:

1. **Disabling unwanted network services**

2. **Flood Ping**

3. **Network sniffing**
   Sniffit
   Ettercap
   Tcpdump

4. **Network monitoring**
   Port scanning (nmap, nessus)
   Traffic monitoring (LAN traffic monitor (iptraf))
   Monitoring changes to Ethernet network cards and IP numbers by users (arpwatch)
   Viewing packets (Dump traffic on a network (tcpdump))

5. **Logging calls and packets**
   Logging packets using NetFilters mechanism and iptables
   External tools for logging packets (IP Protocols Logger (ippl))

6. **Firewall (based on NetFilters and iptables)**
   Packet filtering
   Creating your own strings

7. **Proxy servers**
   WWW Proxy (Squid)

8. **Encrypting connections (Cryptography)**
   SSLwrap
   SSH and SCP

SSH Tunelling

9. **Spoofing**
   Obtaining information about the owner of the IP address and domain

10. **Notifying the relevant authorities about the violation of law**

Methodology:

- PowerPoint mini lectures
- working on computers (each participant works on a separate computer)
- mini training videos

Organizational information:

Number of training hours: 14 hours / 2 days
Time of training 9:15-16:15
Place of training: Łódź, Piotrkowska 125 – KM Studio - trainings