

„Linux – bezpieczeństwo sieci”

Opis szkolenia:

Szkolenie Linux – bezpieczeństwo sieci przeznaczone jest dla administratorów systemów Linux i administratorów sieci, chcących zapoznać się z technikami zabezpieczeń sieci w systemie Linux. Uczestnicy szkolenia Linux – bezpieczeństwo sieci powinni posiadać elementarną wiedzę dotyczącą systemu Linux i sieci w tym systemie.

Program szkolenia:

1. **Wyłączanie zbędnych usług sieciowych**
2. **Flood Ping**
3. **Podglądanie połączeń (Sniffing)**
 - Sniffit
 - Ettercap
 - Tcpdump
4. **Monitorowanie sieci (Network monitoring)**
 - Skanowanie portów (nmap, nessus)
 - Monitorowanie ruchu (LAN traffic monitor (iptraf))
 - Monitorowanie zmian kart sieciowych ethernet oraz nr IP przez użytkowników (arpwatch)
 - Przeglądanie pakietów (Dump traffic on a network (tcpdump))
5. **Logowanie połączeń i pakietów (Logging packets)**
 - Logowanie pakietów z wykorzystaniem mechanizmów NetFilters oraz iptables
 - Zewnętrzne narzędzia do logowania pakietów (IP Protocols Logger (ippl))
6. **Firewall (na bazie NetFilters oraz iptables)**
 - Droga pakietu przez filtry
 - Tworzenie własnych łańcuchów

7. **Serwery proxy**
WWW Proxy (Squid)
8. **Szyfrowanie połączeń (Cryptography)**
SSLwrap
SSH and SCP
SSH Tunelling
9. **Spoofing**
Pozyskiwanie informacji o właścicielu adresu IP oraz domeny
10. **Powiadamianie odpowiednich organów o naruszeniu prawa**

Metodologia:

- mini wykłady w Power Point
- ćwiczenia przy komputerach (każdy uczestnik pracuje na osobnym komputerze)

Informacje organizacyjne:

Ilość godzin szkolenia: 14 godzin / 2dni

Godziny szkolenia: 9:15-16:15

Miejsce szkolenia: ul. H. Sienkiewicza 22, 90-114 Łódź - KM Studio - szkolenia