UNIX/Linux – bezpečnosť dát, bezpečná komunikácia a šifrovanie

Kód kurzu: UNIXB2

Kurz je určený pre správcov sieťových serverov, ktorí potrebujú zabezpečiť ako dáta na serveri, tak aj komunikáciu so serverom. Účastníci sa zoznámia so základmi šifrovania v oblasti počítačovej bezpečnosti. Ďalej sa naučia prakticky používať systémy PGP (GnuPG), SSL, DM-Crypt atď.

Pre koho je kurz určený

Kurz je určený pre správcov siete a sieťových serverov s OS Unix, ktorí sa chcú naučiť zabezpečiť komunikáciu týchto serverov so svojím okolím.

Čo Vás naučíme

Účastníci kurzu sa naučia základným princípom kryptológie a šifrovanie v prostredí počítačovej bezpečnosti. Ďalej sa naučia prakticky implementovať systémy PGP. (GnuPG), SSL atď.

Požadované vstupné znalosti

Dobrá znalosť OS Unix.

Študijné materiály

Študijný materiál GOPAS.

Osnova kurzu

Základné princípy, metódy a aplikácie kryptológie

- Prehľad a použitie bežných kryptologických algoritmov - HASH funkcie, symetrické/konvenčné a asymetrické metódy
- HASH funkcie, prehľad vlastností a použitia (MDx, SHAx atď.)
- Symetrické metódy, prehľad vlastností a princíp fungovania týchto algoritmov, použitie (DES, 3DES, AES atď.)
- Asymetrické metódy, prehľad vlastností a princíp fungovania týchto algoritmov, použitie (DH, RSA, DSA atď.)
- Niektoré vybrané aplikácie, digitálny podpis, vzťahy dôvery - certifikáty atď.

Praktické aplikácie kryptológie

- Systém PGP (GnuPG), použitie
- Systém SSL/TLS, implementácia OpenSSL
- Práca s kľúčmi a certifikátmi
- Program Stunnel
- Šifrované disky pomocou CryptoLoop a DMCrypt

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk