

Linux - bezpieczeństwo systemu

Zabezpieczanie konsoli fizycznej

Zabezpieczenie przed przypadkowym restartem CTRL+ALT+DEL
Zapobieganie startowaniu jądra z dodatkowymi parametrami
Automatyczne wylogowywanie sesji
Blokowanie konsoli wirtualnej

Upgrade systemu

Prawa i własność

Umask
SUID
Sticky bit

Linki twarde (Hard links)

Bezpieczeństwo systemów plików

Mountowanie partycji z dodatkowymi parametrami
Ustalanie rozmiarów partycji oraz systemu plików
Limity pojemności dla użytkowników (quota)

Backup systemu

Sprawdzanie spójności danych (Data integrity checking)

MD5sum
TRIPWIRE

Bezpieczne usuwanie plików

Secure delete (s) attribute
Secure undelete (d) attribute
Wymazywanie danych bez możliwości ich odzyskania (Wipe)

Szyfrowanie systemu plików (Filesystem encryption)

Cryptoloop device

Szyfrowanie i podpisywanie plików (File signing and encryption)

Program GnuPG
Program PGP

Login accounting

Process accounting

Zarządzanie dziennikami systemowymi (Program and kernel messages logging)

Logowanie zdalne (Remote logging)

Zabezpieczanie plików dziennika (Securing logfiles)

Zabezpieczanie przed fałszowaniem plików dziennika (Preventing log tampering)

Alternatywne systemy logowania (Next generation syslog)

Monitorowanie plików dziennika (Log monitoring)

Inne formy monitoringu systemu (Log files and other forms of monitoring)

Łamanie haseł systemowych (Cracking passwords)

Autoryzacja i logowanie do systemu (login i PAM)

Bezpieczeństwo systemu a jądro

OpenWall

GetRwoted

LIDS

RBSAC