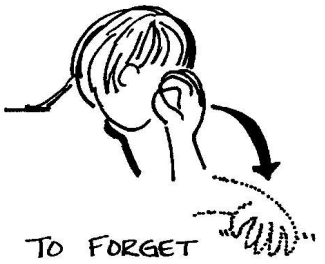
Bezpečnosť v Linuxe

IF:~$ **Rastislav Macko**
macko@netsektor.net

Čo sa dnes dozviete

- Ochrana dát pred zlyhaním techniky
- Hackeri vs. Crackeri
- Vdialené riadene útoky
- Firewally a IDS
- Lokálne útoky
- Patche do jadra
- Šifrovanie
- Ukážka útoku

Majme na pamäti



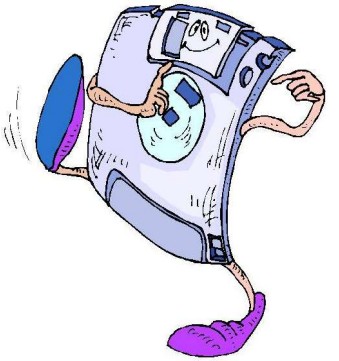
- Ktorý počítač je 100% bezpečný ?
  - nepripojeny k sieti
  - vypnutý

- O čo sa teda snažíme ?
  - to čo mame urobiť dnes, urobiť už včera
  - max. komplikovať utočnikom život
  - kľudne zálohovane v noci zaspávať
  - byť paranoik

Pred čím sa brániť ?

- Poruchovosť hardwaru
- Neočakávane výpadky systému
- Hromadné šírenie nebezpečných programov
- Útoky vedené na diaľku
- Lokálne útoky
- Blbosť uživateľou

Zálohovať !!!



- Tar+gzip
  - tar cfz soubor.tar adresar/
- Rsync
  - rsync local_dir user@host:remote_dir
- Mkisofs
  - mkisofs -J -o image.iso local_dir
- Cdrecord
  - cdrecord dev=1,0,0 -blank=fast image.iso
- Cron
  - crontab -e

Hacker vs.Cracker

- Hacker
  - posadnutý, nadšený prográmator
  - zaľuby: skúmanie a bádanie dokonalosti rôznych typov techlógií
  - typické: vlastný jazyk, jedlo, historia, zmysel pre humor, operačný systém, nepriatelia
  - NESPÁJAŤ s počitačovou kriminalitou !!!
- Cracker
  - spiders,attackers, vandals
  - mladí zvedaví ľudia
  - zaľuby: škodiť, ničiť, rušit súkromie, zneužívať získane informácie

Prečo to robia ?

- Chcú vašu linku
  - zneužitie cudzieho stroja na nabúranie sa do iného systému (anonymita)
- Chcú váš procesor
  - zneužitie procesorového času k vlastným výpočtom.
- Chcú váš disk
  - zneužitie diskového priestoru pre ukladanie vlastných, večšinou nelegálnych dát
- Chcú vaše data a osobné údaje
  - získanie dôvernych informácii (napr. certifikáty)

Dôležitejšie ...

- Chrániť sa pred napadnutím zvonku ?
  - zabezpečovať služby
  - firewally
  - IDS (Intrusion Detection System)
- Chraniť sa pred lokálnym napadnutím ?
  - systémove konta
  - IDS (Intrusion Detection System)
  - ACL (ACcess Lists)
  - Exploity a rootkity
  - prava súborov a adresárov

Zabezpečenie služieb

- Pozor na defaultne nastavené účty !
  - rootovske heslo pre mysql daemon
- Pozor na defaultne spustené služby po inštalácií !
  - služby echo a chargen
- Sledovanie aktuálnych bezpečnostných chýb používaných služieb !

Firewally

- IPchains (starší) a IPtables (nový)
- IPtables – stavový firewall
  - rozoznávanie stavov príslušných spojení
  - tzv. packet filtering
  - označovanie packetov
  - prepisovanie packetov
  - nastavovanie limitov
  - zahadzovanie a odmietanie packetov (rozdiel ?)
  - závislosť na routrovaní
  - voľba defaultnej politiky
  - tzv. connection tracking
  - ...

Záplaty do jádra

- Nedostatočne navrhnutý systém
- Riešenie na úrovni jadra
- Kompromis medzi funkčnosťou a bezpečnosťou

- Najznámejšie projekty:
  - LIDS (www.lids.org)
  - GR security (www.grsecurity.org)
  - RSBAC (www.rsbac.org)
  - Medusa DS9 (http://medusa.fornax.sk)

Práva

- 3 prístupové práva
  - read, write, execute
- vlastníci a skupiny
- nadradený superuživateľ – tzv. root
  - problem s jeho všemocnosťou
  - totálna deštrukcia systému
- Sticky bit
  - neberú sa do úvahy nadradené práva
  - napríklad adresár /tmp
- Atributy súborov (iba pre ext2, lsattr - chattr)
  - pridávanie, komprimovanie, nepozmeniteľnosť, zachovanie obsahu pri odstráneni alebo jeho úplne odstánenie

Intrusion Detection System

- Stražny pes systému
- Prava ruka administrátora
- Projekty:
  - Snort (www.snort.org)
  - PortSentry
  - SHADOW (www.nswc.navy.mil/ISSEC/CID)
- Testovacie nástroje
  - nmap (www.insecure.org/nmap)
  - nessus (www.nessus.org)
  - ethereal (www.ethereal.com)

7 hriechov roota

- Nebezpečné slabé heslá
  - John the Ripper (www.openwall.com/john), knihovna cracklib
- Otvorené sieťové porty
  - NFS, finger, rsh, rlogin, rexec, chargen ... => netstat
- Staré verzie softwaru
  - konferencie
- Chybne nakonfigurované programy
  - FTP, DNS server, Apache
- Chybne stanovené priority
- Zastaralé a nepotrebné účty
  - find / -user ferko -ls, /etc/passwd
- Zabezpečenie je až na prvom mieste

Šifrovanie

- Neprenášať dôverne data nešifrovanie
- Hrozba tzv. útoku man-in-middle
- Nahradiť nešifrované služby za šifrované
  - telnet -> ssh
  - ftp -> ftps alebo sftp
  - imap -> imaps
  - pop3 -> pop3s
- Nepoužívať programy, u ktorých sa zadávaju hesla priamo do konzole – smbclient, pop3client
  - hrozba videnia hesla cez ps iným užívaťeľou

Ďakujem za pozornosť

- www.hackerslab.org
- www.zone-h.org
- www.web-hack.ru
- www.securityfocus.com
- www.linuxsecurity.org