

Tendențe actuale în securitatea Linux

Dragoș Acostăchioaie

<http://www.unixinside.org>

dragos@unixinside.org

Introducere. Cat de importanta este securitatea informatica

- **Vulnerabilitate** = o slabiciune a unui sistem hardware sau software care permite utilizatorilor neautorizati sa obtina acces asupra sa
- numarul vulnerabilitatilor este in crestere: in 2006, CERT raporta 8.064 vulnerabilitati descoperite, in crestere cu 26% fata de anul precedent, iar numarul creste an de an
- numarul de publicatii din 2006 referitoare la vulnerabilitati este in crestere cu 32% fata de anul precedent
- se acorda o importanta din ce in ce mai mare securitatii informatice

Introducere. Cat de importanta este securitatea informatica

- tehnologiile informatice si infrastructurile de comunicatii devin din ce in ce mai integrate in structurile organizatiilor
- utilizarea Internetului in domenii vitale si in scopuri comerciale a crescut potentialul de risc al informatiilor
- protejarea informatiilor a devenit o activitate foarte importanta

Tendinte actuale – Linux vs Windows

- Se observa o scadere semnificativa a utilizarii Windows in favoarea Linux, pentru servere, in special pentru servicii Internet
- marii producatori au renuntat chiar la a oferi Windows ca alternativa pentru anumite modele de servere
- unul dintre motive este ca platforma Linux ofera securitate sporita

Tendinte actuale – atacuri ale sistemelor Linux si Windows

- cu ajutorul *honeypot*-urilor, se pot realiza statistici privind atacurile
- numarul de atacuri impotriva sistemelor Linux, iar perioada de rezistenta a acestora a crescut
- timpul de rezistenta a sistemelor Windows este in continua scadere, cu toate imbunatatirile aduse in domeniul securitatii
- cu cat versiunea de distributie Linux este mai recenta, cu atat perioada de rezistenta (= grad de securitate) este mai mare

Tendinte actuale – atacuri ale sistemelor Linux si Windows

- unele versiuni de distributie Linux nu au fost afectate de perioada efectuarii testelor
- unele dintre sistemele Windows au fost atacate cu succes dupa doar cateva minute!
- motivele acestor rezultate sunt, in principal:
 - numarul mare de probleme de securitate ale sistemelor Windows
 - raspandirii mare a acestor sisteme

Tehnologii actuale in securitatea Linux

- Atacuri indreptate nu impotriva sistemului Linux, dar avand ca suport serverul de

Linux:

- viermi (*worms*)
- virusi trimisi prin e-mail
- atacuri de tip *phishing*
- atacuri de tip *spam*

- Aceste atacuri pot fi combatute prin:

- programe antivirus pentru serverul SMTP (*Clamav, BitDefender* etc.)
- filtrarea e-mailurilor (*SpamAssassin* etc.)

Tehnologii actuale in securitatea Linux

- Atacuri indreptate nu impotriva sistemului Linux, dar avand ca suport anumite servicii de pe serverul Linux:
 - atacuri impotriva serverelor Web
 - *Denial Of Service* (DoS) pentru diferite servicii de retea (DNS, Samba etc.)
- *Rootkit*-uri
 - evolutie a conceptului de cal troian
 - este un pachet de utilitare sistem de tip cal troian, programe aditionale (snifere etc.) si module nucleu (extrem de periculoase)
 - pot fi descarcate de pe Internet!

Tehnologii actuale in securitatea Linux

- *Rootkit*-uri

- isi poarta numele nu pentru ca permit spargerea contului *root*, ci pentru ca ajuta la mentinerea accesului la acest utilizator
- sunt greu de depistat fiindca se bazeaza pe increderea administratorului in utilitarele sistem
- sunt alcatuite, de obicei, din programe precompilate si scripturi de instalare
- alte *rootkit*-uri contin insa fisiere in format sursa

Tehnologii actuale in securitatea Linux

- *Rootkit*-uri

- utilitarele sistem si daemonii au comportament identic cu programele originale
- programele aditionale sunt snifere, programe de criptare, scripturi, utilitare pentru transferul de fisiere etc.
- modulele de nucleu inlocuiesc apeluri de sistem, schimbandu-le adresa
- exista utilitare pentru detectia *rootkit*-urilor, dar pot fi depistate si dupa anumite urme sau monitorizand fisierele importante din sistem

Tehnologii actuale in securitatea Linux

- Utilizarea *honeypot*-urilor pentru detectia si prevenirea atacurilor
 - sunt mecanisme pentru detectia, respingerea si prevenirea incercarilor de utilizare neautorizata a sistemelor informatice
 - are natura unei “capcane” care deruteaza atacatorul
 - au si rol de studiere a atacurilor
- Utilizarea SSL/TLS pentru securitatea informatiilor vehiculate de aplicatii
- Criptarea informatiilor, inclusiv a intreg continutului sistemelor de fisiere
- Utilizarea GPG/PGP pentru protejarea e-mailurilor

Tehnologii actuale in securitatea Linux

- Realizarea de retele private (VPN) pentru a asigura securitatea datelor vehiculate in cadrul organizatiilor
- utilizarea de VPN-uri si *firewall*-uri pentru retelele *wireless* (care conecteaza numeroase dispozitive mobile, in multe organizatii)

Tehnologii actuale in securitatea Linux

- Au aparut numeroase dispozitive care ruleaza Linux, dar care nu ofera un nivel adecvat de securitate
 - routere, multifunctionale, centrale telefonice, PDA-uri etc.
 - multe asemenea dispozitive utilizeaza versiuni vechi de distributii Linux
 - in configuratia initiala au probleme mari de securitate
- Exista solutii integrate de securitate pentru organizatii (hardware/software)