Imbunatatirea securitatii cu ajutorul *honeypot*-urilor

Dragos Acostachioaie

http://www.unixinside.org

dragos@unixinside.org

Definitie. Ce sunt *honeypot*-urile?

- *honeypot* = mecanism pentru detectia sau respingerea incercarilor de utilizare neautorizata a sistemelor informatice
- are natura unei “capcane”
- tehnologia *honeypot*-urilor – nou aparuta, din ce in ce mai des utilizata
- natura *honeypot*-urilor variaza de la un tip la altul
- de cele mai multe ori consta intr-o resursa informatica (document, baza de date, serviciu de retea, server etc.)
- resursa este doar in aparenta parte a sistemului, ea fiind izolata si protejata
- *honeypot*-ul nu are valoare pentru utilizatorii obisnuiti
- interactiunea cu *honeypot*-ul este o activitate neautorizata

Avantaje si dezavantaje

Avantaje ale utilizarii *honeypot*-urilor:

- *honeypot*-urile colecteaza informatii doar atunci cand o persoana sau o aplicatie interactioneaza cu acestea
- sunt generate mai putine date, putand fi mai usor de analizat
- se reduce numarul de alarme false, deoarece *honeypot*-ul interactioneaza doar cu activitatile neautorizate (incercarile de atac)
- sunt flexibile, putand avea numeroase naturi

Definitie. Ce sunt *honeypot*-urile?

Dezavantaje ale utilizarii *honeypot*-urilor:

- induc un factor de risc in cadrul sistemului, deoarece il expun potentialelor atacuri
- *honeypot*-urile sunt specializate pe un anumit tip de interactiune cu atacatorii, cum ar fi conexiunile HTTP sau SMTP
- posibilitatea de a fi usor detectate, deoarece au un comportament constant

Tipuri de *honeypot*-uri

Clasificarea *honeypot*-urilor

- clasificarea dupa gradul de activitate care este permisa cu atacatorul
  - *honeypot*-uri cu interactiune scazuta, care emuleaza servicii de retea sau componente ale unui sistem de operare (usor de instalat, mai sigure, dar colecteaza mai putine informatii)
  - *honeypot*-uri cu interactiune sporita, care simuleaza toate aspectele unui sistem de operare (pot fi integral compromise, permitand efectuarea altor atacuri; colecteaza cantitati mari de informatii)

Tipuri de *honeypot*-uri

- clasificarea dupa modul de conectare la Internet
  - *honeypot*-uri fizice, care constau intr-o masina conectata la retea, avand propria adresa IP
  - *honeypot*-uri virtuale, care sunt simulate de o singura masina, care raspunde la traficul efectuat catre ele

Solutii software pentru *honeypot*-uri

Solutii software *open-source*

- *Honeyd* – daemon care creaza masini virtuale
  - poate fi configurat pentru a emula diferite servicii de retea si pentru a simula un anumit sistem de operare
  - sit proiect - http://www.honeyd.org
- alte proiecte:
  - Nepenthes - http://nepenthes.mwcollect.org
  - honeytrap - http://honeytrap.sourceforge.net

Cercetarea atacurilor. *Honeynet*-uri

Honeynet = *honeypot*-uri cu scop de cercetare a atacurilor din Internet

- sunt *honeypot*-uri cu interactiune sporita si prezinta un risc ridicat
- reprezinta retele de calculatoare, oferind atacatorilor tinte false care simuleaza servicii de retea
- trebuie luate masuri speciale pentru ca in cazul compromiterii sistemelor componente, acestea sa nu poata fi utilizate pentru a ataca alte sisteme
- prin studiul atacurilor pot fi determinate instrumentele si metodele de atac, precum si metodele de comunicare, organizare si motivatiile atacatorilor

Concluzii

- *honeypot*-urile nu reprezinta solutia universala pentru detectia si prevenirea atacurilor
- atacatorii au inceput sa caute metode de depistare si ocolire a *honeypot*-urilor
- *honeypot*-urile pot imbunatati securitatea sistemelor si sprijini cercetarea in domeniul atacurilor informatice
- mai multe informatii:

  http://www.honeypot.net

  http://www.honeynet.org