ELOSZTOTT BEHATOLÁSÉRZÉKELŐ RENDSZEREK LEHETŐSÉGEI, GYAKORLATI FELHASZNÁLÁS

Gyimesi Judit

Konzulensek:

Dr. Fehér Gábor, egyetemi adjunktus, BME-TMIT

Korn András, doktorandusz, BME-TMIT

Networkshop 2005

Bevezető

- Behatolásérzékelő rendszerek - IDS
- Elosztás lehetőségei
- Konkrét probléma: férgek
- Megoldás algoritmusa
- Teljesítményelemzés
- Konklúzió

Behatolásérzékelő rendszer
Intrusion Detection System (IDS)

- Szoftveres, vagy hardveres rendszerek, melyek automatizálják a hálózatban, vagy rendszerben lévő események monitorozását, támadásra utaló jeleket keresve
- Feladatuk a már elkezdett behatolás, támadás felismerése
- Reakció: naplózás, riasztás, beavatkozás
- Más hálózatbiztonsági eszközök kiegészítéseként (pl. tűzfal a gyanús forgalom tiltására)

Adatfeldolgozás módszere

- Szabály alapú IDS / Anomália alapú IDS
- normális viselkedés modellje (pl. statisztika alapú)
  - küszöbértéknél nagyobb eltérés
  - viselkedésmodell frissítése időközönként
- Hátránya: kijátszható, sok téves riasztás (párhuzamos megoldás kell)

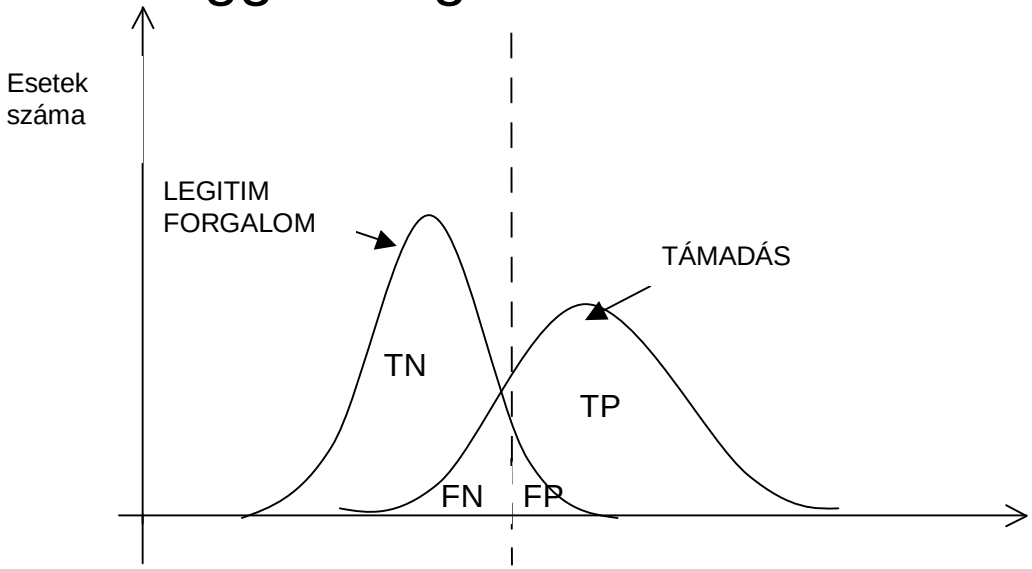
  Előnye: **ismeretlen támadások** szűrhetőek, automatizálás

Probléma: Féreg támadás

- Egy, vagy kevés gépről indul
- Az IP térben a féreg által kihasznált sebezhetőséggel rendelkező gépek keresése
  - véletlenszerűen, vagy előzetes tudás alapján
  - hatékonyabbak a saját alhálózattal kezdik
- Fertőz: átküldi a kódját a sebezhető célra
- Az utóbbi két lépést időnként megismétli (pl. minden újraindításkor)
- Ilyenkor kis időn belül sok csomag kerül kiküldésre

Megoldás: Elosztott IDS-ek

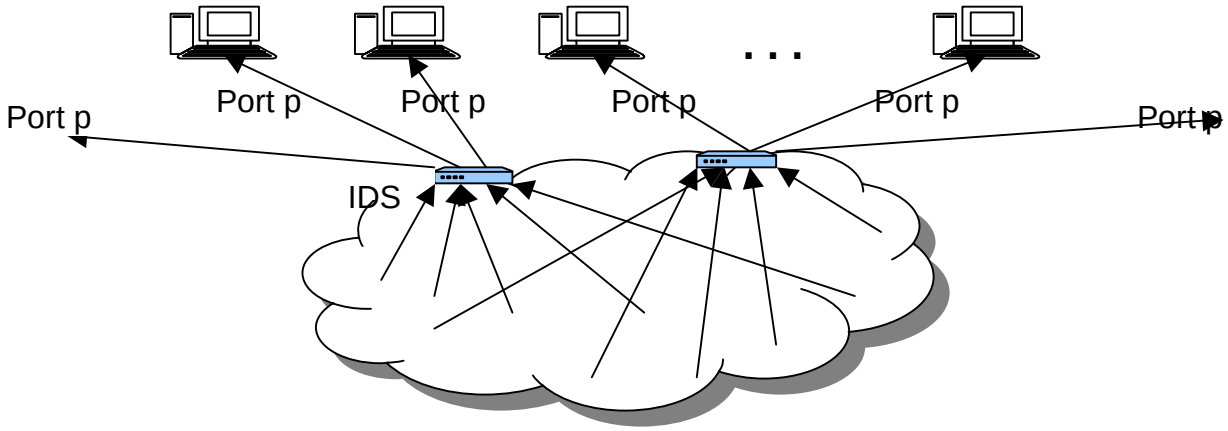
- Egyetlen IDS csak korlátozott forgalomnövekedést lát
- Ha több IDS egyszerre észlel mérsékelt növekedést, együtt már gyanús
- Az elosztás jelen esetben lehetővé tesz nagyobb biztonsággal meghozott döntéseket



Féreg felismerési elve

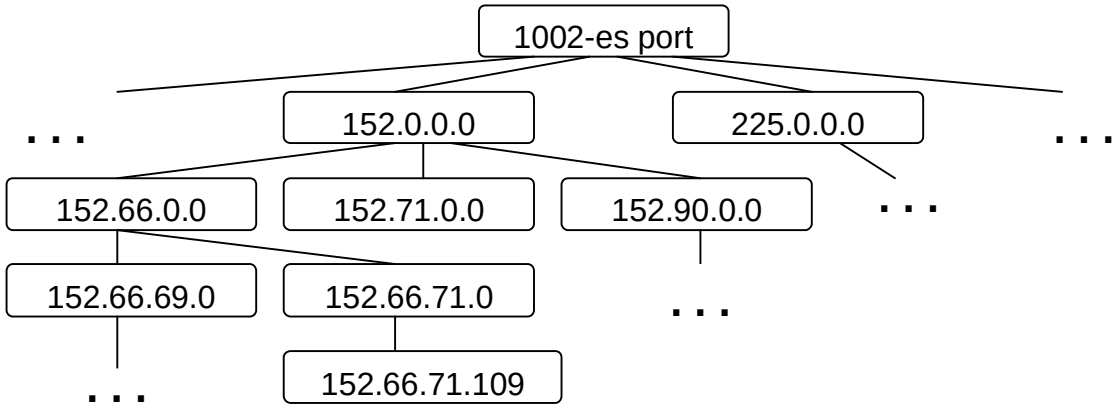
- Nem amikor az alhálózat gépe(i) fertőződik, hiszen az csak pár csomaggal jár
- Továbbterjedésnél. Azonos portra tartó forgalom megnövekedése (különböző forrás- és célcímek)

  Statisztika-alapú anomália-detekció
- Általában az első támadási hullám kevésbé védhető, a kikapcsolt és elszigetelt gépek azonban menthetőek.



Az algoritmus

- Csomagtípust (célport, célcím) pár jellemez
- Minden célporthoz statisztika tárolása
- Monitorozáskor az IDS minden célporthoz tárol egy fát, ami azokból a célcímekből áll, amely cím azonos portjára küldtek csomagot.
- Minden beérkező csomagra beszúrás művelet, ha nincs ilyen csomópont
- Anomália mértékét az alsó szint leveleinek száma adja.



Az algoritmus (folyt.)

- Időintervallumonként törlés
- Elosztott anomália-detekció:

  minden IDS-nek saját normális statisztika, küszöbértékek

  1. Alsó küszöbérték alatt: legitim forgalomnak veszi.
  2. Felső küszöbérték fölött: önálló cselekvés
  3. A kettő között lekérdezi a többi IDS megfigyeléseit is.
- Reakció felismert féregtámadás esetén a kérdéses forgalom teljes azonnali tiltása, operátor riasztása, és naplózás lehet.

Analízis (I.)

- Jelölések:

  n – az érték, amit a vizsgált IDS az adott támadás esetén felmerülő porthoz tárol

  Δt – megfigyelési időintervallum

  $k1$, $k2$ – alsó ill. felső küszöbérték

  t – ennyi idővel egy intervallumkezdet után kezdődik a terjedés

  φ – a féregterjedés csomagszáma egy időintervallumban

Analízis (II.)

Feltételezések:

- a terjedés egyenletes csomagforgalmat generál
- fertőzött gépek egyszerre kezdenek csomagokat küldeni
- Nem feltételeztem hálózati architektúrát, az ehhez kapcsolódó paraméterek implicit vannak jelen
  - hosztok, fertőzött hosztok száma helyett csak generált forgalom
  - IDS-ek száma helyett egy átlagos értéket, hogy egy csomagot hány IDS lát

Analízis (III.)

- Az architektúra reakcióideje akkor különbözik az egyes IDS-ekétől, amikor kommunikációra kerül sor. Ennek feltétele:

$$k_1 \le \frac{n+j}{n} \le k_2$$

- A kommunikáció kezdete a leggyorsabb IDS felismerési ideje
- Ezután ha T idő alatt zajlik le a kommunikáció, és ezalatt már sorban tiltanak le az IDS-ek, akkor a reakcióidő közelítése:

$$\frac{(\Delta t - t)}{\Delta t} j_1 + \frac{k_1 n_1}{j_1 + n_1} j_1 + ((\Delta t - t) + \frac{k_1 n_1}{j_1 + n_1} \Delta t) \frac{j}{\Delta t} + T \frac{j}{2\Delta t}$$

- Egy átlagos architektúrában azonban egyetlen csomagot több IDS is fog látni, ezért ennek az értéknek csak az arányos hányada jelent különböző csomagot.

Példa

- Legyen Δt =15perc=900s,
  φ=800 csomag/900s,
  t=850s
  T=2s
- A leggyorsabb IDS-re pedig
  k11=1.2, k21=10,
  φ1=200 csomag/900s
  n1=50 csomag/900s
- A becslés szerint maximum 49 új fertőzés lehetséges.

Az elosztott IDS-ek lehetséges egyéb felhasználási területei:

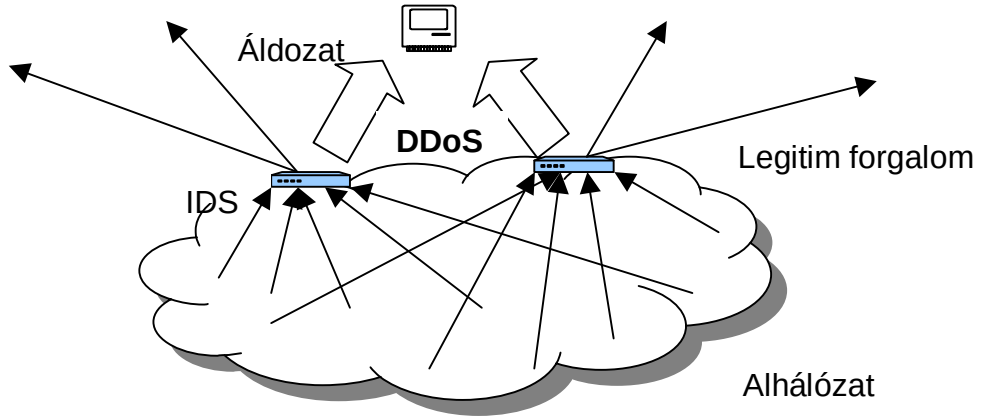
- A férgek összehangolásakor fellépő, fertőzött gépek közötti kommunikáció észrevétele
- Jóval gyorsabb reakció az olyan portok esetében, amelyekre nem, vagy alig érkezik legitim forgalom.
- A módosított eredmény tehát

$$(j + T\frac{j}{2\Delta t})$$

- Ami az előző körülményeknél 4 csomagot jelent.

További lehetőségek:

- Portscan felismerése:
  A férgek felismeréséhez hasonló elv alapján
- Kimenő DDoS támadás felismerhető



- Költségek csökkentése: egy alhálózatban az egyes forgalmak helyett aggregált monitorozás

Ezen megoldás-lehetőségek alapelvei

Ezekben az esetekben is megnövekedett forgalmat vizsgálhatunk, az alábbi jellemzőjű csomagtípusokra:

Támadás típusa	*Figyelt jellemzők*	*Várt megfigyelések*
(D)DoS	célcím	1 célcím
portscan	célcím, célport	1 célcím, sok célport
férgek	célcím, célport	sok célcím, 1 célport

Konklúzió

- Újfajta védekezés a férgek ellen
- Hatékonyság matematikai analízisre alapozva
- Továbbfejlesztési elvek
- Az elosztott architektúra a detektálás biztonságát javítja, anélkül a téves riasztások megengedhetetlenül nagy száma miatt lehetetlen lenne a felismerés.

Köszönöm a figyelmet!