Honeypotok & Honeynetek

Dr. Unicsovics György

e-mail: gy.unicsovics@nbh.hu

HTE előadás, Budapest **2008. november 3.**

Áttekintés:

- Mi is az a Honeypot és a Honeynet?

- Kereskedelmi forgalomban elérhető alkalmazások.

- Honeypotok és az igazságügyi vizsgálatok.

- Honeypotok detektálása.

- A jövő.

Mi a Honeypots?

A honeypot egy IT eszköz, melynek elsődleges értéke a törvény és más felhasználói jogok által nem engedélyezett rendszerhozzáférések megakadályozásában található .

- Nincs produktív értéke; minden ami ki /be érkezika honeypotba az egy próba és a támadások kiszűrésére, kompromittálására szolgál;

- Támadások monitorozására, detektálására és elemzésére használatos;

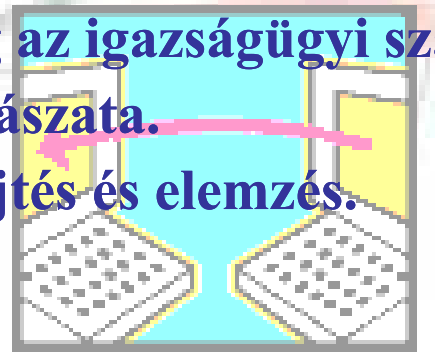
- Nem old meg speciális problémákat, flexibilis eszköz, amely együttműködik különböző biztonsági alkalmazásokkal.

Miért Honeypots?

Mert ez egy nagyszerű eszköz az IT biztonsági szakemberek és magának az IT világ számára.

Honeypots:

- Beépített anti-virus aláírások.
- Beépített SPAM aláírások és filterek.
- ISP-ka kompromittálódott megállapítására.
- Kellő segítség az igazságügyi szakértők részére.
- Botnetek vadászata.
- Malware gyűjtés és elemzés.



A probléma!

Az Internet és az IT hálózatokbiztonsága komplex és bonyolult kérdés

- Naponta új támadási formák;

- Az IT hálózatok statikus célpontot jelentenek;

-Mit tehetünk?

Minél jobban megismerjük ellenségeinket, annál jobban építhetjük ki védelmi rendszerünket!!!

- Hamis célpontok alkalmazása?

A Honeypotok osztályozása:

Interakció szintje alapján:

- **Magas;**
- **Alacsony;**
- **Közepes ?**

Megvalósítás alapján:

- **Virtuális;**
- **fizikai;**

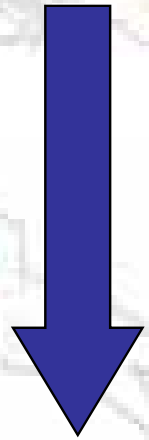
Célok alapján:

- **Termék;**
- **Forrás.**

Kereskedelmi forgalomban hozzáférhető Honeypotok:

Alacsony interakció

BackOfficer
DTK
HOACD
Honeynets



Magas interakció

Mi a Honeynet?

Magas interakciójú Honeypot:

- Mélységi információk gyűjtésére szolgál;

- figyeli, ki mikor és hogyan akar a rendszer felhasználójává válni a rendszergazdák engedélye nélkül.

- Ez architektúra!!!

- nem egy termék vagy egy szoftver.

- Élő rendszerre települ;

- Kinézhet, úgy mint egy aktuális termék.

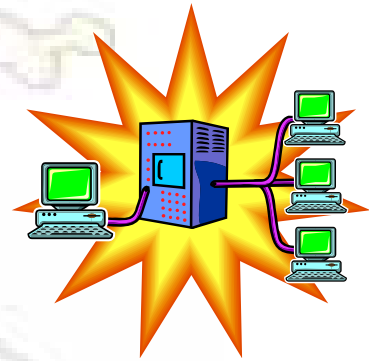
Mi a különbség a Honeypot és a között Honeynet?

- **Honeypot→ sérülékenységek felderítésére.**
  - ***Egyszerű konfigurácó, speciális szoftverrel, vagy emulációval;***
  - ***ki, mikor és hogyan támadja a rendszerünket;***

- **Honeynet → a hálózat megnyitása támadások indikálása céljából**
  - ***Rendszer szoftverrel együtt, alapértelmezésben telepítve;***
  - ***Tűzfal mögött;***
  - ***Jobb ha a honeynet megy tönkre, mint az élő rendszer.***

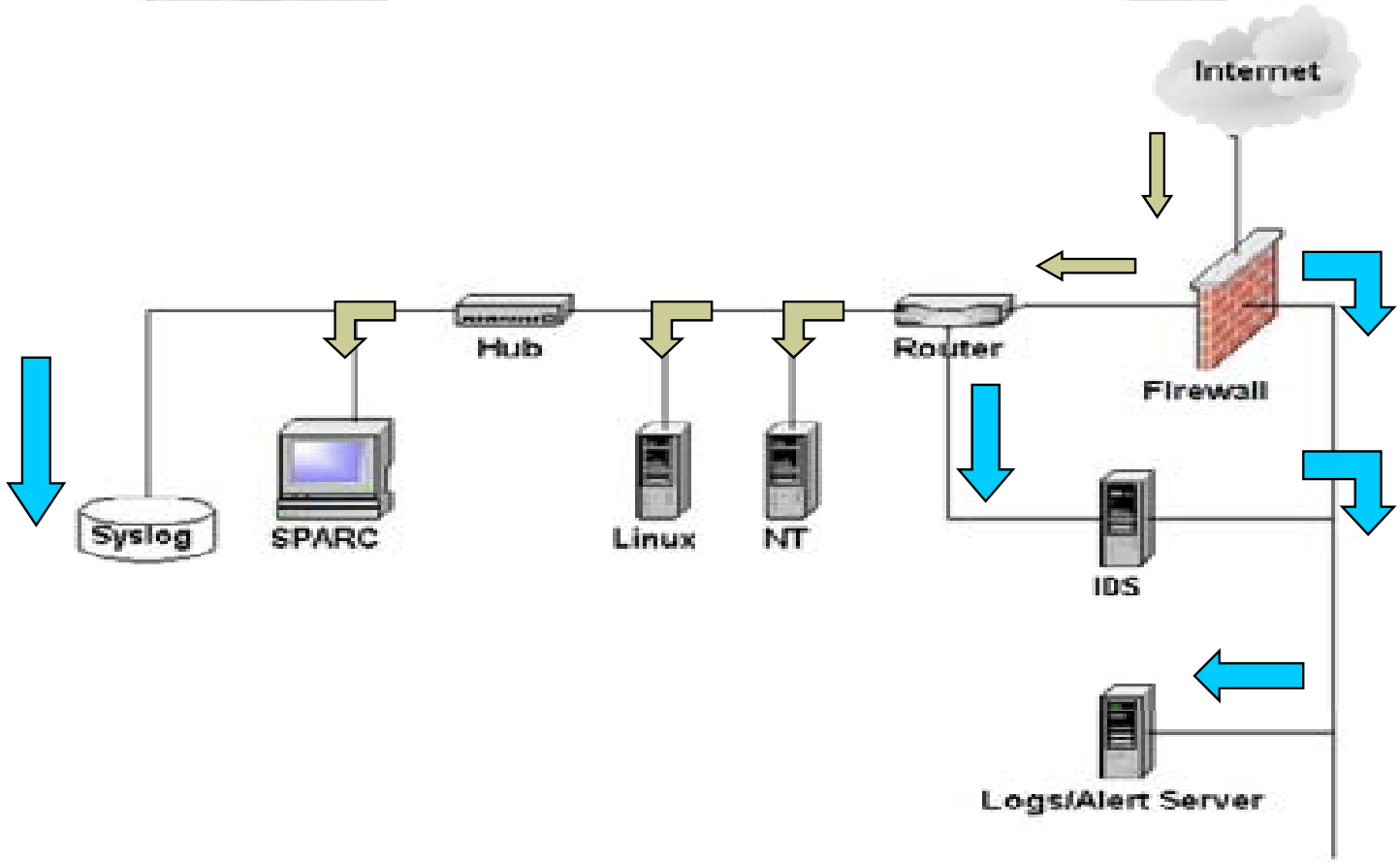
Hogy működik?

- Szigorúan ellenőrzött hálózat, ahol minden egyes csomag függetlenűl annak irányától, vizsgálatra kerül;
  - Ellenőrzés;
  - Elfogás;
  - Elemzés;

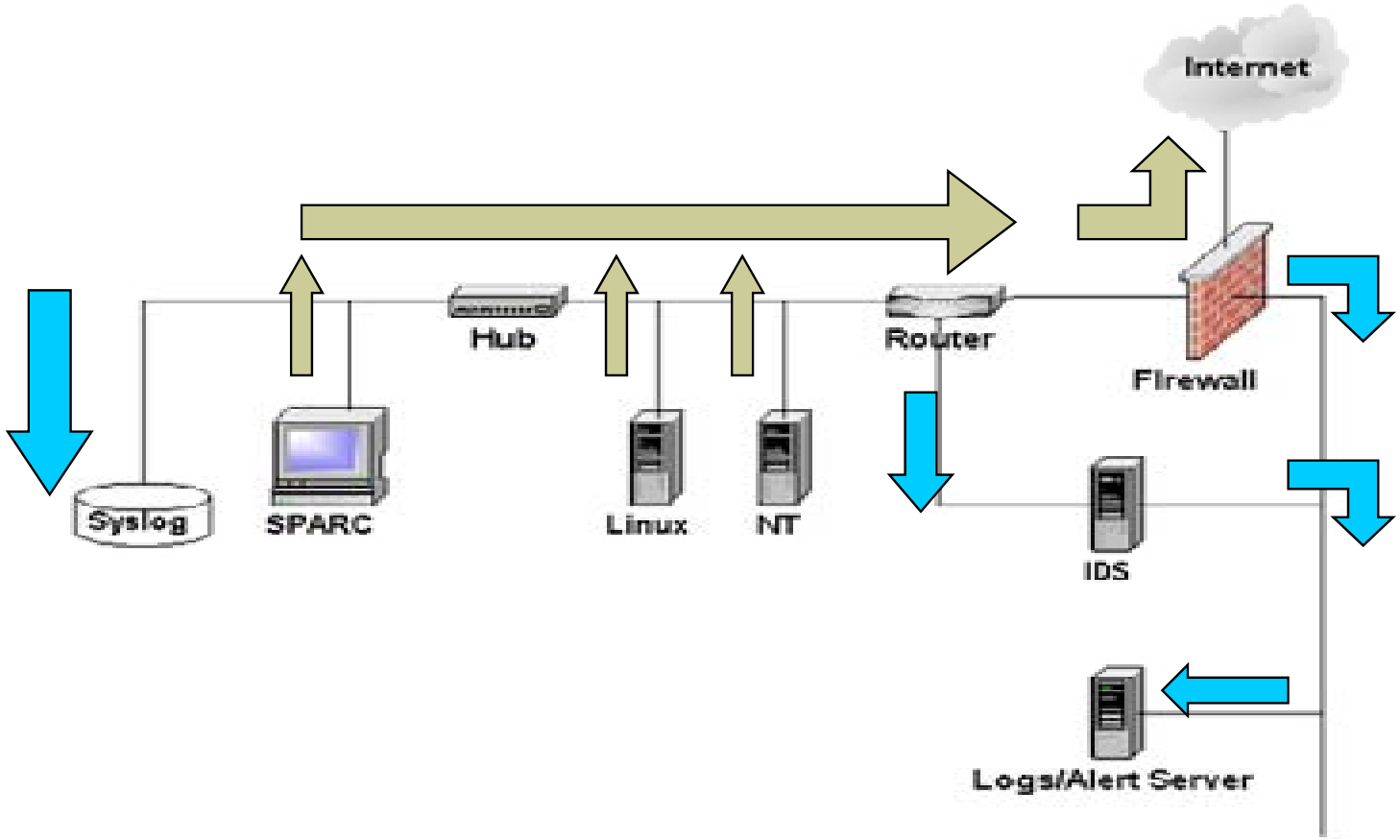


- Minden csomag amely érinti a Honeynetet, természeténél fogva gyanusnak tekintendő;

Honeynet diagramm



Honeynet diagramm



Honeypot és az igazságügyi vizsgálatok

- Azt igazságügyi szakértők bíróság előtt megálló bizonyítékokat keresnek...., ilyenek a különböző számítógépes rendszerekből kinyert adatok (azonosítók, dokumentumok és a meta adatok, stb.);

- A honeypot technológia legbonyolultabb része, ez sokszor több mint tudományos próba;

- Jegyezzük meg! Mindig tartsuk evidenciában a vonatkozó jogszabályokat amikor Honeypotot telepítünk;
  - Engedély nélküli felhasználás;
  - Bűnözés elősegítése;
  - Magántulajdon és az adatvédelmi törvény megsértése.
  - ...

Honeypot és az igazságügyi vizsgálatok folyt.

• Világos és jól behatárolt metódus a vizsgálatok során; - Eredeti bizonyítékok minden változtatás nélkül (lehetőleg elfedve minden adatszerzésre irányuló tevékenységünket!)

- A megszerzett adatok integritásának ellenőrzése;
- Az elemzés értékelés végrehajtása az eredeti dokumentum módosítása nélkül;

• Minden vizsgálat kulcsa:

- alternatív dokumentációk készítése (fotók, jelentések).

Honeypot és az igazságügyi vizsgálatok folyt.

(eltünő és maradandó információk)

- **Eltünő információk: RAM-ban tárolt infók (futó alkalmazások, memória tartalmak, nyitott fájlok, hálózati kapcsolatok, jelszavak, stb.) eltűnnek amikor a gép kikapcsolásra kerül;**

- **Maradandó információk:A számítógép kikapcsolása után is megmaradó információk (HDD tárolt adatok);**

- **A lényeges kérdés: Mi a helyzet az eltünő információkkal az igazságügyi vizsgálatok során?**

Honeypot és az igazságügyi vizsgálatok folyt.

(eszközök az eltünő információk kinyerésére)

- **Biztonságos média felhasználása (hordozható eszközök) a bizonyítékok begyűjtése során;**

Unix/Linux:

- ps, netstat, ifconfig, date, grep, last, cat, ls, lsof, mount, dd, fdisk, …

Microsoft Windows:

- netstat, ipconfig, VICE, diskmon, filemon, handle, listdlls, process explorer, pstools, regmon, tcpview, tdimon, tokenmon, livekd, dir, …

Soha ne tároljuk a kinyert információkat a lokális rendszerünkön!!!!

Honeypotok detektálása

- Technicai tulajdonságok
  - Válaszidő, banners, registry bejegyzések, inkonzisztens paraméterek;
- "Social" tulajdonságok, felhasználói interakció
  - Nem tipikus (pl. nincs új file a rendszerben heteken keresztül…);
- Network sniffing
  - Csomagok ki/be a rendszerben (a szimatolás végrehajtását a hálózat egy másik rendszeréből tegyük);
- Nyomok keresése a Vmware-ben
  - A Vmware népszerű alap, bár lokálisan könnyen detektálható;

Honeypotok detektálása folyt.

- Honeypot eszközök nyomainak keresése:

  Temp mappák, kernel dumps, backdoors (sebek etc.)

- History analízise

  Nem csak a „rossz fiúk” követnek el hibákat

-A Honeypotnak magának a sérülékenysége (alacsony, vagy közepes interakciójú honeypot esetén)

- KREATIVITÁS!!!

Honeypotok jövője

-Honeytokens;

-Wireless honeypots;

-SPAM honeypots;

-Honeypot farms;

- Search-engine honeypots.

Honeypotok jövője

-Új honeypot detektálási technológiák;

-Automatizált honeypot scannerek és“zavarók”;

- Anti Honeypot Technológiák;

- Honeypot exploits.

Konklúzió

- Honeypot nem egy probléma megoldás, hanem egy flexibilis eszköz, amely különböző alkalmazásokkal együtt szolgálja az IT rendszerek biztonságát;

- Elsődleges értéke az információgyűjtés területén van;

- Megfelelő idő a működéshez;

- Soha ne töltsünk fel valós adatokat;

- Soha ne kapcsolódjunk amikor Honeypotunk aktív!!!

További információk:

- *http://www.honeynet.org/*
- *http://www.honeynet.org/book*