The Honeynet PROJECT

# *Betörés megelőző rendszerek*

*Molnár Zoltán Vilmos*

*2003.12.03*

The Honeynet PROJECT

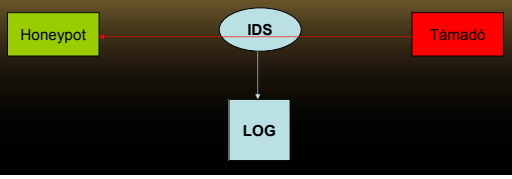
## Témák

- Elméleti áttekintés
- Betörés megelőző rendszerek működése
- Betörés megelőző rendszer építése nyílt forrású rendszerekkel

The Honeynet PROJECT

## Mi az IDS?

*(Intruding Detection System)*




The Honeynet PROJECT

## Mire használhatjuk az IDS-t?

- Egy úgynevezett virtuális gépet (Honeypot) elérhetővé teszünk, és elemezzük a hozzá beérkező töréseket.
- Ezeket az adatokat felhasználva az igazi rendszerünket védhetjük a behatolóktól.

The Honeynet PROJECT

## Mi az IPS?

*(Intruding Providing System)*


The Honeynet PROJECT

## Fontosabb szempontok

- Az IDS és IPS rendszereknek láthatatlannak kell lennie, így a hálózaton csak adatkapcsolati szinten lehet jelen.
- Ha feltörnek egy virtuális gépet, akkor a hacker/cracker ne tudjon arról támadást indítani

The Honeynet PROJECT

## Jogi következmények

Az adott rendszerekért a rendszergazdák a felelősek. Minden általuk karbantartott gépről induló támadásért ők felelnek, hacsak:

- A rendszergazda mindent megtesz az érdekében, hogy ne lehessen feltörni a rendszert, és ezt bizonyítani is tudja.

The Honeynet PROJECT

## Témák

- Elméleti áttekintés
- Betörés megelőző rendszerek működése
- Betörés megelőző rendszer építése nyílt forrású rendszerekkel

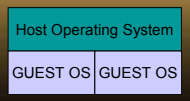
The Honeynet PROJECT

## I. Generációs Honeynet

- Az arp táblát módosítva a „*honeyd*” démon virtuális eszközöket hoz létre a hálózaton.
- A gépeket Layer3 tűzfal mögé rejtjük és NAT-ot alkalmazunk. A kimenő forgalmat szabályozzuk.

The Honeynet PROJECT

## I. Generációs Honeynet




The Honeynet PROJECT

## Példa a detektálásra, és módosításra

alert tcp $EXTERNAL_NET any -> $HOME_NET 53
msg: ”DNS EXPLOIT named”; flags: A+;
keret tartalma:”|CD80 E8D7 FFFFFF|” – (/bin/sh)
keret módosítva: ”|0000 E8D7 FFFFFF|” – (/ben/sh)

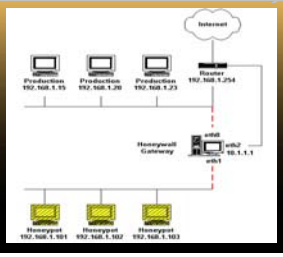
The Honeynet PROJECT

## II. Generációs Honeynet

- A virtuális gépeket egy úgynevezett „*Firewall-Bridge*” –el kötjük össze. A gépek felé irányuló forgalmat naplózzuk.

The Honeynet PROJECT

## II. Generációs Honeynet




The Honeynet PROJECT

## A Firewall-Bridge működése


The Honeynet PROJECT

## Témák

- Elméleti áttekintés
- Betörés megelőző rendszerek működése
- Betörés megelőző rendszer építése nyílt forrású rendszerekkel

The Honeynet PROJECT

## I. Generációs Honeynet építéséhez használt szoftverek

- Honeyd démon
- Arpd démon
- Naplózási rendszer (pl.: sebek2, snort)
- rc.firewall script
- Unix/Linux rendszer

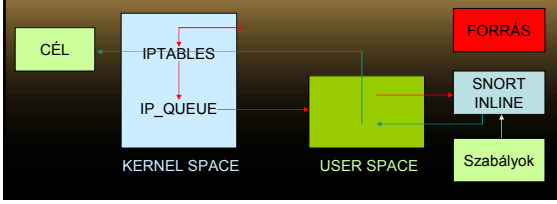
The Honeynet PROJECT

## II. Generációs Honeynet építéséhez használt szoftverek

- User-Mode-Linux
- Kernel patch a Firewall-Bridge támogatáshoz
- Bridge-utils
- rc.firewall script
- Snort-Inline

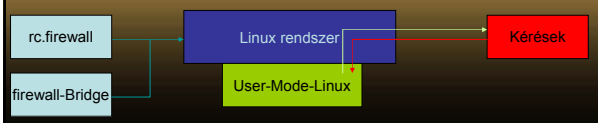
The Honeynet PROJECT

## II. Generációs Honeynet Kernel működés




The Honeynet PROJECT

## II. Generációs Honeynet építéséhez használt szoftverek



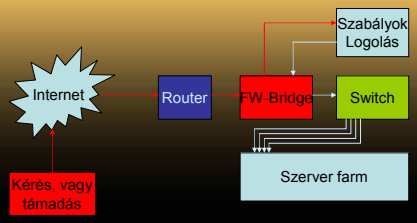

The Honeynet PROJECT

## II. Generációs Honeynet telepítése

- Elsőként készítsük fel kernelünket a Firewall-Bridge és a TAP hálózati meghajtó támogatására (Networking Options, Network Devices)
- Installáljuk fel az User-Mode-Linux-ot.
- Állítsuk be az rc.firewall-t.
- Installáljuk fel a Snort-Inline programot.
- Fogalmazzuk meg a szabályokat a Snort-Inline programban.

The Honeynet PROJECT

## IPS rendszer megépítése




The Honeynet PROJECT

## IPS rendszer megépítése

- A legfontosabb szempont, hogy a Firewall-Bridge csak a döntéshozó és naplózó gépekkel legyen IP szinten összekötve!!!
- A Routert érdemes tűzfalra cserélni, és csak a számunkra fontos portokat továbbítani a célszerver felé.

The Honeynet PROJECT

## Összefoglalás

- Cél: megvédeni a számunkra fontos adatokat illetéktelenektől.
- Eszközök: megismerni az ellenséget, és így védekezni ellenük, intelligens hálózati eszközök használatával.
- Következtetés: A nyílt forrású rendszerek használata kellőképpen biztonságos.
- Végkövetkeztetés: Aki attól fél állandóan, hogy éppen most törik a rendszerét az paranoiás, aki abban a hitben él, hogy a rendszere feltörhetetlen, az felelőtlen!

The Honeynet PROJECT

## Köszönöm a figyelmet!

*Várom a kérdéseket!*