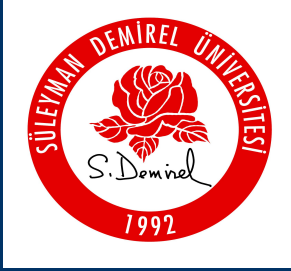


HONEYD KURULUMU



K. Koray ÜÇTOP

Süleyman Demirel Üniversitesi

Bal Küpü Tuzağı (Honeypot) ve Kara Delik (Black Hole)
Çalışma Grubu

http://www.honeyd.org

Developments of the Honeyd Virtual Honeypot - Mozilla Firefox

Doğya Düzen Görünüm Geçmiş Yer İmleri Araçlar Yardım

http://www.honeyd.org/ openoffice şablon

Pardus Pardus Durakları Wikipedi Bilgi Sorgulama Bankalar Haberler Özgür Yazılım Diğer Açık Dizin

Proxy: None Apply Edit Remove Add Status: Using No Proxy Preferences

openoffice şablon - Google... [Pardus-kullanicilari] Open... Developments of the Hon... Ulak-CSIRT

Monkey.org Developments

Developments of the Honeyd Virtual Honeypot

Honeyd Resources

- [Main](#) - [News](#) - [Forums](#) - [New](#)
- [Download Releases](#)
- [General Information](#) ([Mirror](#))
- [Frequently Asked Questions](#)
- [Sample Configurations](#)
- [Tools](#) - [Service Scripts](#)
- [Live Statistics](#) - [New](#)
- [Links, Press, etc.](#)
- [Mailing List Archive](#)
- [Acknowledgments](#)

Honeyd Research

- [Immunization Against Worms](#)
- [Understanding Spam](#)
- [Performance](#)

Honeypot Resources

- [Honeypot Background](#)
- [Honeypot Concepts](#)

Happy Hacking

- [Reduce wishlists](#)
- [Leave a tip with PayPal](#)

Support Honeyd

- [Support Honeyd](#)

HONEYD DEVELOPMENT

Honeyd is a small daemon that creates virtual hosts on a network. The hosts can be configured to run arbitrary services, and their personality can be adapted so that they appear to be running certain operating systems. Honeyd enables a single host to claim multiple addresses - I have tested up to 65536 - on a LAN for network simulation. Honeyd improves [cyber security](#) by providing mechanisms for threat detection and assessment. It also deters adversaries by hiding real systems in the middle of virtual systems.

Honeyd is open source software released under GNU General Public License. Even though Honeyd is used commercially by many companies, it is being developed in my spare time without any financial support. Nonetheless, I always appreciate a *reduction of my wishlists*, if you feel so inclined. The README in Honeyd's source distribution and the [acknowledgments](#) page lists a number of people who have contributed code and ideas.

Current Status

Honeyd is maintained and developed by [Niels Provos](#). **Honeyd 1.5b** has been released on 2006-08-19 and the next version is currently being developed.

Reporting Bugs and Source Code

Bugs can be reported via [Google Code](#). Honeyd source code can be accessed via [subversion](#).

Forums

[Discussion forums](#) for [news](#) and [general interest](#) items are now available.

Tam... 2,250s Proxy: None kazkoru@gmail.com Şu anda: Kısmen güneşli, 7° C Paz: 8° C Pzt: 11° C

13:18

Sistem ve Gereksinimler:

Kullanılan sistem :

Amd 3200+
512 Mb RAM
80 Gb Hdd
Centos 4.4 i386 (Server kurulum+X+Güncellemeler)

Gereksinimler :

libpcap (İşletim sistemi kurulumunda hazır)
libdnet (<http://libdnet.sourceforge.net>)
libevent (<http://www.monkey.org/~provos/libevent-1.3b.tar.gz>)
arpd (<http://www.citi.umich.edu/u/provos/honeyd/arpd-0.2.tar.gz>)
honeyd (<http://www.citi.umich.edu/u/provos/honeyd/honeyd-1.5b.tar.gz>)

Centos 4.4 için kurulum:

`http://dag.wieers.com/rpm/`

Dag deposu Redhat, RHEL, Centos ve Fedora için rpm paketleri sunar.

```
$ rpm -Uvh http://apt.sw.be/packages/rpmsforge-release/rpmsforge-release-0.3.6-1.el4.rf.i386.rpm
```

komutu ile repoyu sisteminize ekleyebilirsiniz. Bu işlemden sonra sırasıyla;

```
$ yum update  
$ yum install honeyd
```

komutları ile “honeyd” sisteme kurulur. “libevent” honeyd kurulumu sırasında bağımlılık gereği kuruluyor.

Sorun!

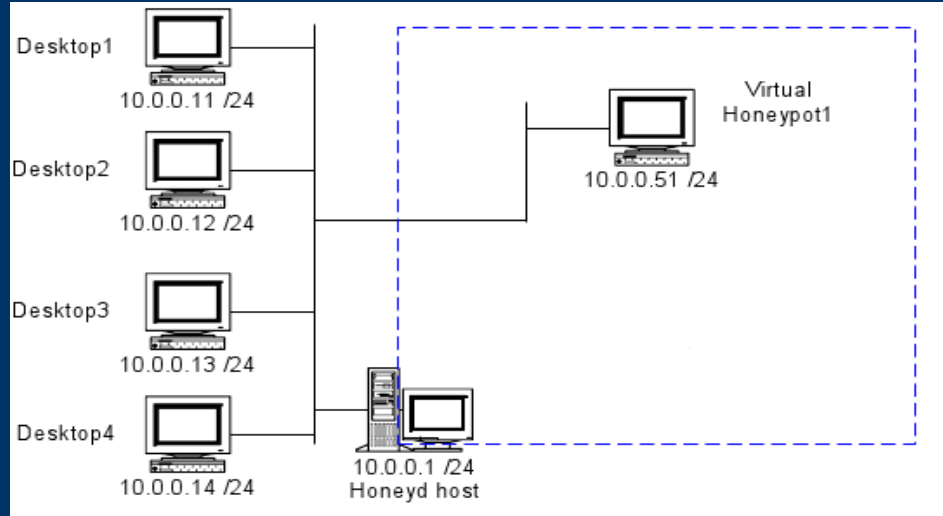
arpd ve honeyd farklı libevent sürümlerini kullanıyor.

Çözüm!

```
$ arp -s 192.168.x.x Mac-adresi pub
```

komutu ile statik arp girdisi kullanılabilir.

Honeynet in oluşturulması:

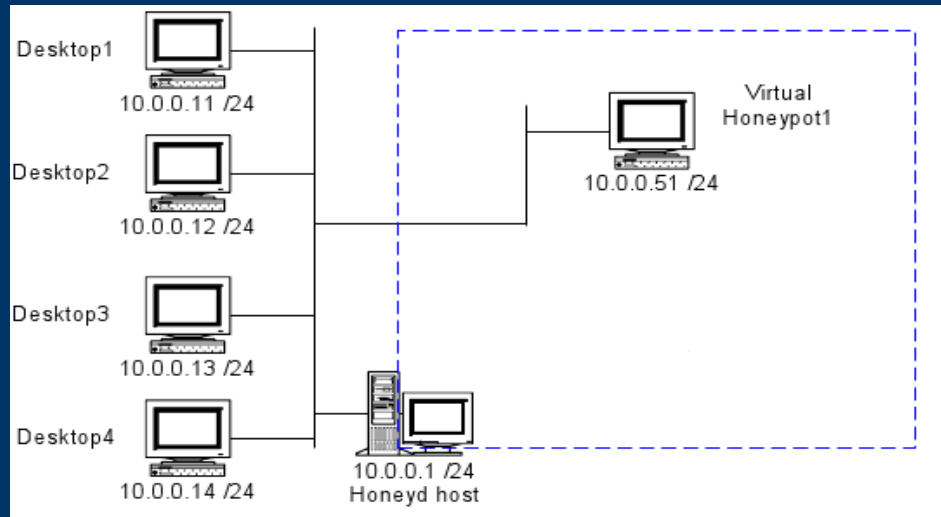


Oluşturulacak sanal honeypotlar ve honeynet yapısı için “honeyd.conf” dosyasındaki komutlar işlenir. Örnek konfigürasyon dosyaları için, <http://www.honeyd.org/configuration.php> adresinden faydalanılabilir.

Ayrıca, http://www.citi.umich.edu/u/provos/honeyd/honeyd_kit-1.0c-a.tgz adresindeki toolkit içerisinde derlenmiş arpd, honeyd ve kullanılacak örnek konfigürasyonlar ile çeşitli servislerin emülasyonu için betikler bulunmaktadır.

```
$ arp -s 10.0.0.51 <ethernetin Mac adresi> pub (oluşturulacak honeypot için)
```

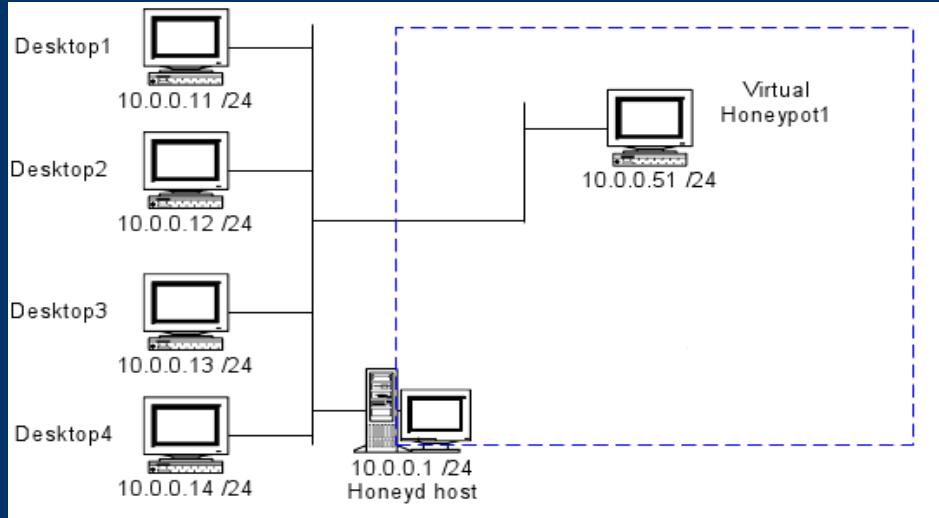
Honeynet in oluşturulması:



Oluşturulabilecek basit bir honeypot için "honeyd.conf" dosya içeriği,

```
create winxp
set winxp personality "Microsoft Windows XP Professional SP1"
set winxp uptime 319671
add winxp tcp port 80 "perl scripts/win32/iis-0.95/iiseml8.pl"
add winxp tcp port 139 open
add winxp tcp port 137 open
add winxp udp port 137 open
add winxp udp port 135 open
set winxp default tcp action reset
set winxp default udp action reset
bind 10.0.0.51 winxp
```

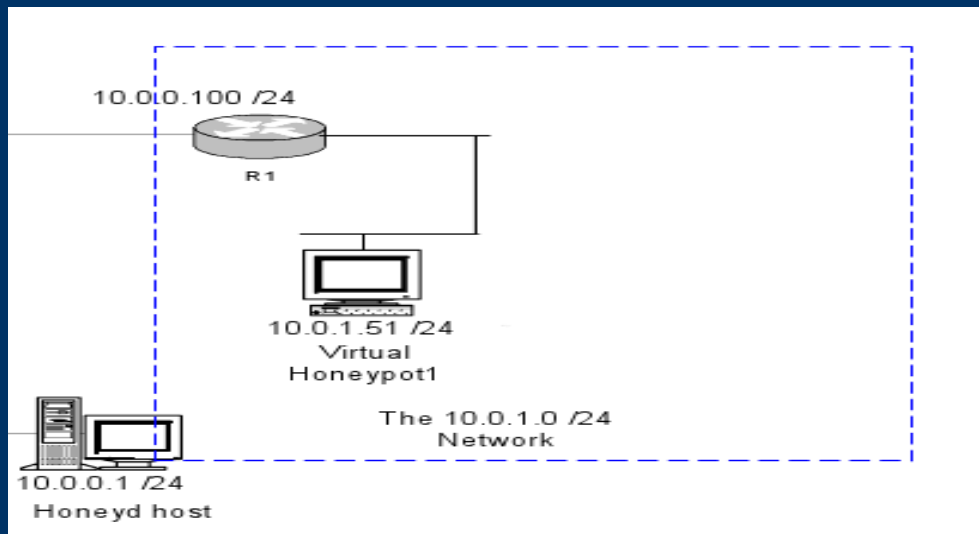
Honeynet in oluşturulması:



Tutulacak günlük dosyası için istenilen bir klasörde dosya oluşturulup yazma ve okuma izni verildikten sonra sıra “honeyd” yi çalıştırmaya gelir.

```
$ honeyd -f honeyd.conf -l honeyd.log -i eth0
```

Honeynet in oluşturulması:



Oluşturduğumuz honeynet'e bir de router eklemek istersek, önce router için arp tanımlaması yapılır.

```
$ arp -s 10.0.0.100 <ethernetin Mac adresi> pub
```

Ardından "honeyd.conf" dosyasına aşağıdaki satırları eklemek yeterli olacaktır.

```
create cisco
set cisco personality "Cisco 1601R router running IOS 12.1(5)"
add cisco tcp port 23 "perl scripts/router/cisco/router-telnet.pl"
set cisco default tcp action reset
set cisco default udp action reset
set cisco uid 32767 gid 32767
set cisco uptime 1327650
bind 10.0.0.100 cisco
```

Honeynet in oluşturulması:

Tutulan günlük dosyası izlendiğinde,

```
$ tail -f honeyd.log
```

Aşağıdaki örneğe benzer satırlar görülebilir.

```
2004-01-07-14:36:58.7132 tcp(6) - 252.214.169.203 2064 192.168.27.180 21: 48 S [MacOS 8.0-8.6 OTTCP]
2004-01-07-15:26:40.0209 tcp(6) - 244.233.22.102 61891 172.162.8.180 21: 60 S [FreeBSD 5.0-5.1 ]
2004-01-07-16:48:30.1212 tcp(6) S 192.168.21.135 33395 172.162.8.91 80 [Linux 2.6 ]
2004-01-07-16:48:41.4929 tcp(6) S 10.173.240.67 22110 192.168.14.178 81 [Windows XP SP1]
```

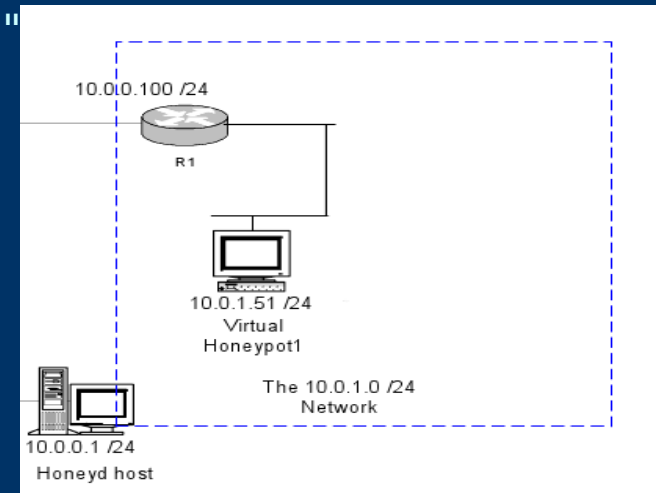
Bu satırlardaki önemli anahtarlar;

- İlk kısımda, olayın gerçekleşme tarih ve zamanı belirtir. (2004-01-07-14:36:58.7132)
- İkinci kısımda, olayın gerçekleştiği protokolü belirtir. (tcp(6))
- Üçüncü kısımdaki S harfi yeni bir bağlantının başladığını, E harfi bağlantının sonlandığını belirtir.
- Dördüncü kısımda ise, <src ip, src port, dst ip, dst port> şeklinde bağlantı bilgilerini belirtir.
- Beşinci ve son kısımda ise, bağlantıyı gerçekleştiren işletim sistemi hakkında bilgi verilir.

Honeynet in oluşturulması:

```
create winxp
set winxp personality "Microsoft Windows XP Professional SP1"
set winxp uptime 319671
add winxp tcp port 80 "perl scripts/win32/iis-0.95/iiseml8.pl"
add winxp tcp port 139 open
add winxp tcp port 137 open
add winxp udp port 137 open
add winxp udp port 135 open
set winxp default tcp action reset
set winxp default udp action reset
bind 10.0.0.51 winxp
```

```
create cisco
set cisco personality "Cisco 1601R router running IOS 12.1(5)"
add cisco tcp port 23 "perl scripts/router/cisco/router-telnet.pl"
set cisco default tcp action reset
set cisco default udp action reset
set cisco uid 32767 gid 32767
set cisco uptime 1327650
bind 10.0.0.100 cisco
```



Faydalanılan Kaynaklar:

- Honeyd ile network simülasyonu

http://www.paladion.net/papers/simulating_networks_with_honeyd.pdf

- Managing a Honeyd

<http://www.oreilynet.com/lpt/a/6726>

- Honeyview: Log analizi için basit web arayüzlü bir program

<http://sourceforge.net/projects/honeyview/>

- Honeyd

<http://www.honeyd.org/>

- Open Source Honeyd: Learning with Honeyd

<http://www.securityfocus.com/infocus/1659>