

# Ulak CSIRT Balküpü Tuzağı ve Kara Delik Çalışma Grubu

Murat Soysal- Onur Bektaş  
Koray Üçtop

# Bal Küpü (Honeypot) Nedir?

- Bilişim sistemlerine karşı gerçekleşen saldırıların tespit edilmesi için kurulmuş olan tuzaklardır.
- Üzerlerinde saldırganların dikkati çekecek hizmetler sunarlar.(WWW,SMTP vb)
- Saldırıların tespiti ve raporlanması için kullanılırlar.
- Düşük iletişimli (low-interaction) sistemlerdir.

# Balküüpü Ağı

- Balküüpü cihazlarının biraraya gelerek oluşturduğu ağa balküüpü ağı denir.
- Yüksek iletişimli (high interaction) sistemlerdir.
- Kompleks ağ topolojisi oluşturarak gerçek bir ağ yapısını simule ederler.

# Oluşum

- Akademik Bilişim 2007'de grup oluşturulması için çağrı yapıldı.
- UlakNet Forumları (UFO) üzerinden gelen katılma istekleri ile grup oluşturuldu.

# Grup Üyeleri

- Murat Soysal *Ulakbim*
- Hakan Aysal *İstanbul Üniversitesi*
- Koray Üçtop *Süleyman Demirel Üniversitesi*
- Onur Bektaş *Ulakbim*
- Fatih Ertam *Fırat Üniversitesi*
- Hüsnü Demir *ODTÜ*

# Çalışma Grubu Hedefleri.

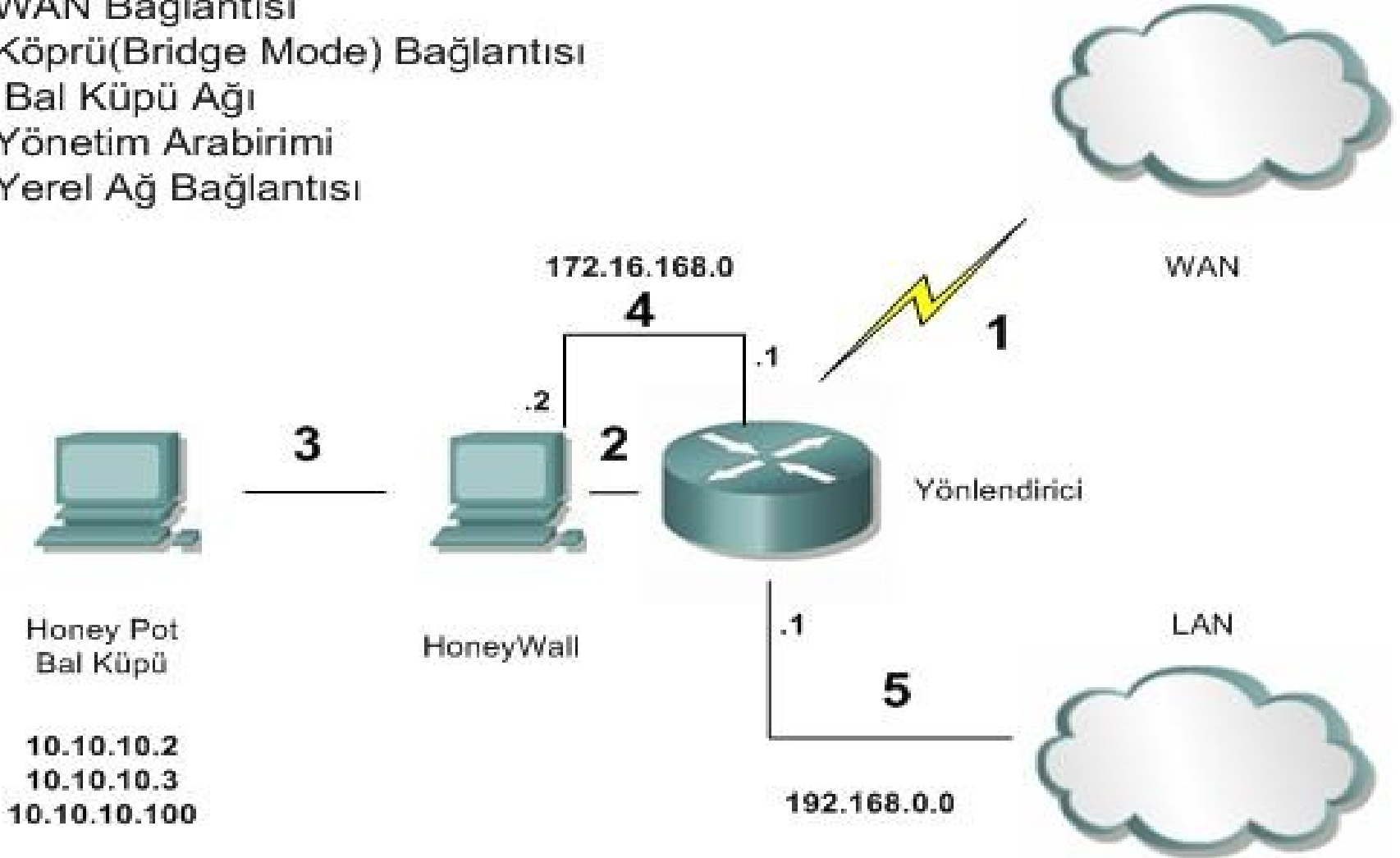
- UlakNet bünyesinde hizmet verecek merkezi bir balküpü sunucusu ile ağ içinde dolaşan şüpheli trafiğin incelenmesi, kaynağının tespit edilmesi.
- Kaynağı tespit edilen saldırıların olay kayıtlarının girilmesi.
- İlk aşamada UlakNet içinden yapılan saldırıların daha sonra UlakNet'e dışarıdan gelen saldırıların sınıflandırılması, raporlanması ve istatistik bilgilerinin verilmesi.
- Balküpü kurulumu ve işletimi ile ilgili dökümantasyon oluşturulması.

# Balküüpü ve Balküüpü ağı programlarının seçimi

- Balküüpü programı
  - Honeyd ([www.honeyd.org](http://www.honeyd.org))
  - En yaygın uygulama.
- Balküüpü ağı programı
  - Honeywall ([www.honeynet.org](http://www.honeynet.org))
  - Honeywall CDROM, Hazır izleme, yönetim, raporlama paketleri.

# Test Yatağı

- 1 WAN Bağlantısı
- 2 Köprü(Bridge Mode) Bağlantısı
- 3 Bal Küpü Ağı
- 4 Yönetim Arabirimi
- 5 Yerel Ağ Bağlantısı



# Iptables Günlüğü (LOG)

- Mar 8 14:08:42 datlum kernel: INBOUND OTHER: IN=br0 OUT=br0 PHYSIN=eth0  
PHYSOUT=eth1 SRC=193.140.82.1 DST=224.0.0.10 LEN=60 TOS=0x00 PREC=0xC0 TTL=2  
ID=0 PROTO=88
- Mar 8 14:08:45 datlum kernel: INBOUND TCP: IN=br0 OUT=br0 PHYSIN=eth0  
PHYSOUT=eth1 SRC=125.77.171.189 DST=193.140.90.170 LEN=64 TO S=0x00  
PREC=0x00 TTL=30 ID=37220 DF PROTO=TCP SPT=4676 DPT=1433 WINDOW=53760  
RES=0x00 SYN URGP=0
- Mar 8 14:08:45 datlum kernel: OUTBOUND TCP: IN=br0 OUT=br0 PHYSIN=eth1  
PHYSOUT=eth0 SRC=193.140.82.205 DST=193.140.94.33 LEN=148 T OS=0x10  
PREC=0x00 TTL=64 ID=59745 DF PROTO=TCP SPT=22 DPT=55016 WINDOW=33304  
RES=0x00 ACK PSH URGP=0
- Mar 8 14:08:46 datlum kernel: INBOUND OTHER: IN=br0 OUT=br0 PHYSIN=eth0  
PHYSOUT=eth1 SRC=193.140.82.1 DST=224.0.0.10 LEN=60 TOS=0x 00 PREC=0xC0  
TTL=2 ID=0 PROTO=88
- Mar 8 14:08:48 datlum kernel: INBOUND TCP: IN=br0 OUT=br0 PHYSIN=eth0  
PHYSOUT=eth1 SRC=86.35.198.93 DST=193.140.90.170 LEN=48 TOS= 0x00  
PREC=0x00 TTL=109 ID=11341 DF PROTO=TCP SPT=4383 DPT=1433  
WINDOW=16384 RES=0x00 SYN URGP=00.90.93 LEN=61 TOS=0x00 PREC=0x00  
TTL=114 ID=41340 PROTO=ICMP TYPE=8 CODE=0 ID=512 SEQ=37438

# Honeyd Günlüğü

2007-03-12-10:19:09.6656 tcp(6) E 193.140.170.50 4882  
193.140.30.87 1433: 41 0

2007-03-12-10:19:09.6676 tcp(6) S 193.140.170.38 2242  
193.140.82.74 1433 [Windows XP SP1]

2007-03-12-10:19:09.6814 tcp(6) - 193.140.170.50 4882  
193.140.30.87 1433: 40 A [Windows XP SP1]

2007-03-12-10:19:09.7256 tcp(6) E 193.140.170.50 4900  
193.140.90.166 1433: 41 0

2007-03-12-10:19:09.7306 tcp(6) S 193.140.170.36 2149  
193.140.125.239 1433 [Windows XP SP1]

2007-03-12-10:19:09.7427 tcp(6) - 193.140.170.50 4900  
193.140.90.166 1433: 40 A [Windows XP SP1]

2007-03-12-10:19:09.8286 tcp(6) E 193.140.170.43 3511  
193.140.35.135 1433: 41 0