Linux ile Ağ Servisleri

ODTÜ BİLGİ İŞLEM DAİRE BAŞKANLIĞI, 2007

ccnet@metu.edu.tr

GİRİŞ

- İşletim Sistemi
  - Kurulum kısmı
  - Güvenlik
  - Çekirdek
  - Log Tutma
- Zebra veya Quagga
- IDS – Snort
- IDS - BASE
- RRDTool ve LOG Tutma
- Sistem Ayarları
- iptables - Örnek
- SON

İşletim Sistemi

- Özgür yazılımlar
  - Bedava mı?
  - Kullanıcı tercihi.
    - BSD tabanlı
    - Linux tabanlı
  - Netfilter Linux işletim sistemlerini ön plana çıkarmakta.
    - BSD çekirdeği 7. seviye istemiyor
- BSD tabanlı makine
  - Çalışma zamanı 460 gün.
  - Performansı gayet iyi.

İşletim Sistemi

- Linux işletim sistemi.
  - Debian tabanlı
    - İşletim sisteminin en önemli noktası çekirdeği.
    - Kişiye en kolay gelen dağıtım seçilmeli.
    - Güncellemeleri takip eden bir dağıtım olsa iyi olur ☺
  - Bir köprü olarak çalıştırdığımız Linux tabanlı bir IDS cihazının en son çalışma zamanı yaklaşık 410 gündü.
- Kararlı bir sürüm yakalandıktan sonra cihaza dokunma.
  - İşletim sisteminde kullanılmayan ve kullanılmayacak özellikler için işletim sistemi güncellenmemelidir.
  - Mesela çekirdekte bir sorun yoksa yeni çekirdek çıktı diye güncelleme yapılmamalıdır.

İşletim Sistemi

- Kullanılan işletim sistemlerine ait web sayfaları takip edilmelidir.
- Kullanıcı listelerine üye olunmalıdır. Aktif olarak katılmak şart değildir.
- Güvenlik siteleri günlük kontrol edilmelidir.
  - http://www.cisecurity.com
  - http://www.nsa.gov
  - http://www.microsoft.com/security
  - http://www.sans.org
  - http://www.eeye.com
  - http://www.securityfocus.com
  - http://www.cert.org
  - http://csirt.ulakbim.gov.tr
- Güvenlik listelerine üye olunmalıdır.

İşletim Sistemi – Kurulum

- Kurulum için kullanılacak cihazın tüm donanımsal özellikleri bir yere not edilmelidir.
- CPU, slot sayısı, tipleri ve hızları, bellek, disk kapasitesi, SCSI, ağ kartı ve tipleri gibi bilgiler toplanmalıdır.
- Bu kartların Linux ile ilgili performans değerleri önceden araştırılmalı. Sorunlu kartlar kullanılmamalı.
- İşletim sistemi ile ilgili kurulum notları okunmalıdır.
- Dağıtıma özel notlar kesinlikle okunmalıdır.

İşletim Sistemi – Kurulum

- Debian **Etch**.
- CD'den veya hatta DVD'den kurmak artık çok kolay.
  - Kurulum için http://www.debian.org.
  - Kurulum sadece BASE ile yapıldı.
  - Kurulum esnasında kurulan çekirdek standarttır.
  - Disk yapılandırması önemlidir.
    - Loglama kendi üzerinde olacaksa performans düşebilir.
  - Kurulum esnasında ağ bağlantısı sağlanırsa kurulumun hızlıca güncellenmesi sağlanır.
    - Kaynak dosyalar güvenilir sitelerden sağlanmalıdır.
  - Şifrenin en az on karakterli ve sağlam olmasını öneririz.

İşletim Sistemi – Kurulum

- Sorun anında ilk önce başvurulacak kaynak:
  - http://www.google.com.tr
- Daha sonra;
  - http://forum.ulak.net.tr
- Son olarak da ilgili dağıtım sitelerine başvurulabilir.
- Kurulum yapıldıktan hemen sonra eğer ağ kablonuz bağlı ise;
  - *# vi /etc/apt/sources.list*
    - **#** *deb cdrom: ……* **satırı comment'lenmelidir.**
  - Eğer yok ise şu satırlar eklenmelidir;
    - deb http://ftp.tr.debian.org/debian/ etch main
    - deb-src http://ftp.tr.debian.org/debian/ etch main
    - deb http://security.debian.org/ etch/updates main contrib
    - deb-src http://security.debian.org/ etch/updates main contrib
  - Sonra "*aptitude update"* ve *"uptitude upgrade"* kullanılmalıdır.

İşletim Sistemi – Güvenlik

- Güvenliği sıkılaştırmak için;

  # iptables –A INPUT –i lo –j ACCEPT
  # iptables –A INPUT –m state --state INVALID –j DROP
  # iptables –A INPUT –m state --state RELATED,ESTABLISHED –j ACCEPT
  # iptables –A INPUT –j DROP
  # iptables –A OUTPUT –j ACCEPT

- */etc/hosts.allow* ve */etc/hosts.deny* dosyaları işlenmelidir. hosts.deny dosyası "*ALL:ALL*" olmalıdır.
- *"ps –ef"* komutu ile çalışan uygulamalar kontrol edilmeli ve istenmeyen uygulamaları son verilmelidir.
  - lpd genelde kullanılmıyor. "*killall lpd*" ve "*update-rc.d –f lpd remove"*

İşletim Sistemi – Çekirdek

- Çekirdek için ilk önce http://www.kernel.org kontrol edilmelidir.
- Daha sonra kernel ftp://ftp.tr.kernel.org adresinden çekilebilir.

```
# cd /usr/src/
# aptitude install ncftp
# ncftp ftp.tr.kernel.org
NcFTP 3.2.0 (Aug 05, 2006) by Mike Gleason (http://www.NcFTP.com/contact/).
Connecting to 144.122.144.146...
Middle East Technical University * Anonymous * FTP Server
Logging in...
Anonymous access granted, restrictions apply.
Logged in to ftp.tr.kernel.org.
ncftp / > cd pub
ncftp /pub > cd linux/
ncftp /pub/linux > cd kernel/
ncftp /pub/linux/kernel > cd v2.6
ncftp /pub/linux/kernel/v2.6 > ls -l L*
-r--r--r--   1 ftp      ftp           0   Nov 29 22:11   LATEST-IS-2.6.19.2
ncftp /pub/linux/kernel/v2.6 > get linux-2.6.19.2.tar.bz2*
linux-2.6.19.2.tar.bz2:                      40.75 MB  256.03 kB/s
linux-2.6.19.2.tar.bz2.sign:                  248.00 B   25.86 kB/s
ncftp /pub/linux/kernel/v2.6 > bye
# gpg --keyserver wwwkeys.pgp.net --recv-keys 0x517D0F0E
# gpg --verify linux-2.6.19.2.tar.bz2.sign linux-2.6.19.2.tar.bz2
gpg: Signature made Wed 10 Jan 2007 05:21:53 PM EST using DSA key ID 517D0F0E
gpg: Good signature from "Linux Kernel Archives Verification Key <ftpadmin@kernel.org>"
Primary key fingerprint: C75D C40A 11D7 AF88 9981  ED5B C86B A06A 517D 0F0E
```

İşletim Sistemi – Çekirdek

 # tar jxf linux-2.6.19.2.tar.bz2
 # ln -s linux-2.6.19.2 linux
 # cd linux
 # less README
 # make mrproper

Eğer eski konfigüraston dosyanız varsa .config olarak bunu kullanabilirsiniz.
 # make oldconfig

Veya yeniden başlamak için;
 # make menuconfig

Genelde kullanma ihtimalimiz olan ama şu an için kullanmayacağız kısımları modül olarak işaretlemede fayda vardır.
Şunlar işaretli olsa iyi olur:
Code maturity level options ---> [*] Prompt for development and/or incomplete code/drivers
Networking ---> Networking options --->
[*] Network packet filtering (replaces ipchains) --->
Core Netfilter Configuration --->
IP: Netfilter Configuration --->
Tamamını Modül olarak işaretleyebiliriz. Ipv6 ile ilgili bir şey yapmayacağız. Kullanılmayan herşeyi geçersiz kılmakta yarar var.
QoS and/or fair queueing --->
Tamamını Modül olarak işaretleyebiliriz.

Device Drivers ---> Network device support --->
Ilgili kartları seçebilirsiniz.

İşletim Sistemi – Çekirdek

- Bundan sonra "*make*", "*make install*" ve "*make modules_install*" komutlarını çalıştırmak yeterli olacaktır.
- Eğer **grub** kullanıyorsanız "*update-grub*" komutunu kullanmanız gerekiyor demektir.
- Her türlü kurulum bilgileri için İnternet yeterli gelmektedir.
- NETFILTER
  - http://www.netfilter.org
  - Eğer ektra özellik istemiyorsak "*aptitude install iptables*" yeterli olacaktır.
  - ipset, ip2p ve l7-filter çok önemli özelliklerdir.
  - QoS ile çok güzel uygulamalar yapılabilmektedir.
    - *Kitap: Designing and Implementing Linux Firewalls and QoS using netfilter, iproute2, NAT, and L7-filter, Lucian Gheorghe, PACKT Publishing, Oct 2006.*

İşletim Sistemi – Log Tutma

- Sistemdeki izleri takip etmek için Cisco tarafından kullanılan Netflow kullanılacaktır.
- Bu izleri toplaması için “*fprobe*” uygulaması kullanılacaktır.
- “*aptitude install fprobe-ng”*
- “/etc/default/fprobe” dosyası içerisindeki INTERFACE ve FLOW_COLLECTOR parametreleri değiştirilir.
  - INTERFACE=eth0
  - FLOW_COLLECTOR=“localhost:5555”
- Günlük verileri toplamak için flow-tools kurulabilir.
- Verileri cihaz üzerinde toplamamak ve merkezi bir sistem oluşturmak hem performans hem de güvenlik için önemlidir.

Zebra veya Quagga

- Zebra, Quagga'nın atası.
- Pekçok bölümden oluşur.
  - IPv6 ve IPv4 olarak ayrılır.
  - zebra uygulaması kernel ile diğer uygulamalar arasındaki iletişimi sağlar. İlk önce çalıştırılmalıdır.
  - *ospfd, ripd, bgpd* gibi uygulamalar çokça kullanılmaktadır.
  - Sınır yönlendiricilerde *bgpd* genelde kullanılmaktadır.
  - Uygulamaların varsayılan çalışma portlarını değiştirmek iyi bir güvenlik önlemidir.
  - Kurulum için

    # aptitude install quagga

    veya

    # wget http://www.quagga.net/download/quagga-0.99.6.tar.gz
    # tar zxvf quagga-0.99.6.tar.gz
    # cd quagga-0.99.6
    # ./configure --disable-ipv6 --disable-ripd --disable-ripngd
    # make
    # make install
    # cd /usr/local/etc/
- Sistemi çalıştırmak için;
  - # /usr/local/sbin/zebra –d –P 4000
  - # /usr/local/sbin/ospfd –d –P 4001

Zebra veya Quagga

```
# less /usr/local/etc/zebra.conf
!
! Zebra configuration saved from vty
!   2007/04/06 10:06:34
!
hostname Router
password zebra
enable password zebra
log file /var/log/zebra.log
!
interface eth0
!
interface eth1
!
interface lo
!
access-list NOLOGIN permit 127.0.0.1/32
access-list NOLOGIN deny any
!
!
line vty
 access-class NOLOGIN
!
```


```
# less /usr/local/etc/ospfd.conf
!
! Zebra configuration saved from vty
!   2006/09/29 14:43:43
!
hostname Router-ospfd
password zebra
enable password zebra
log file /var/log/ospfd.log
!
interface eth0
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 ospf-key
 ip ospf hello-interval 30
 ip ospf dead-interval 120
!
interface eth1
!
interface lo
!
router ospf
passive-interface eth1
 network 10.1.0.0/24 area 0.0.0.0
!
access-list NOLOGIN permit 127.0.0.1/32
access-list NOLOGIN deny any
!
line vty
 access-class NOLOGIN
```

Zebra veya Quagga

- SNMP desteği de kurulum esnasında verilebilir.
- Bu destek ile cihaza doğrudan ulaşıp istatistiksel bilgiler alınabilir.
- Bu bilgiler **rrdtool** ile işlenip grafiksel hale dönüştürülebilir.
  - http://oss.oetiker.ch/rrdtool
- Quagga veya Zebra sistemi “Cisco” komutlarına çok benzemektedir.
  - Bu pekçok kullanım kolaylığı sağlamaktadır.
  - Cihazlar arası geçişte yardımcı olmaktadır.
  - Yeniden eğitim gerekmemektedir.

IDS – Snort

- Yönlendirici cihazda IDS sisteminin bulunması yararlı olmaktadır.
  - Ele geçirilmesi çok büyük bir sorundur.
- INLINE özelliği büyük sistemlerde önerilmemektedir.
  - Performans kaybı
  - "*Herşeyi engelle, gerekli olanlara izin ver*"
  - Para/politika
- Snort sistemi aptitute ile rahatlıkla kurulabilmektedir.
  - http://www.snort.org/docs/setup_guides/deb-snort-howto.pdf adresindeki kurulum gerçekten çok ideal.
    - Sadece apache ile ilgili bir sorunla karşılaşıldı.
  - snort.org sitesine üye olunmalıdır.

IDS – Snort

- *# wget http://www.snort.org/dl/current/snort-2.6.1.2.tar.gz*
- *# wget http://www.snort.org/dl/current/snort-2.6.1.2.tar.gz.md5*
- *# md5sum snort-2.6.1.2.tar.gz*
- *22c448e25538cdf74c62abe586aeac0a snort-2.6.1.2.tar.gz*
- *# cat snort-2.6.1.2.tar.gz.md5*
- *22c448e25538cdf74c62abe586aeac0a snort-2.6.1.2.tar.gz*
- *#*
-
- ***Daha sonra kural dosyalarını indirmek gerekiyor. Snort.org sitesinden kural dosyalarını indirebilmek için REGISTER olmanız gerekmektedir.***
- *# wget http://www.snort.org/pub-bin/downloads.cgi/Download/vrt_os/snortrules-snapshot-CURRENT.tar.gz*
- *# wget http://www.snort.org/pub-bin/downloads.cgi/Download/vrt_os/snortrules-snapshot-CURRENT.tar.gz.md5*
- *# wget http://www.snort.org/pub-bin/downloads.cgi/Download/comm_rules/Community-Rules-CURRENT.tar.gz*
- *# wget http://www.snort.org/pub-bin/downloads.cgi/Download/comm_rules/Community-Rules-CURRENT.tar.gz.md5*
- *# wget http://www.bleedingsnort.com/bleeding.rules.tar.gz*
-
- *# tar zxf snort-2.6.1.2.tar.gz*
- *# cd snort-2.6.1.2*
- *# less RELEASE.NOTES*
- *# less doc/INSTALL*
- *# ./configure --enable-dynamicplugin --enable-pthread*
- *# make*
- *# make install*

IDS – Snort

- ***Sistemi test etmek için;***
- *# snort -evi eth0*
- *Running in packet dump mode*
-
- *--== Initializing Snort ==--*
- *Initializing Output Plugins!*
- *Var 'any_ADDRESS' defined, value len = 15 chars, value = 0.0.0.0/0.0.0.0*
- *Var 'lo_ADDRESS' defined, value len = 19 chars, value = 127.0.0.0/255.0.0.0*
- *Verifying Preprocessor Configurations!*
-
- *Initializing Network Interface eth0*
- *Decoding Ethernet on interface eth0*
-
- *--== Initialization Complete ==--*
-
- *,,_   -*> Snort! <*-*
- *o")~   Version 2.6.1.2 (Build 34)*
- *''''   By Martin Roesch & The Snort Team: http://www.snort.org/team.html*
- *(C) Copyright 1998-2006 Sourcefire Inc., et al.*
-
- *Not Using PCAP_FRAMES*
- *01/22-03:30:58.187791 0:18:FE:78:2D:7C -> 0:11:85:C0:D7:97 type:0x800 len:0x86*
- *144.122.3.141:22 -> 144.122.3.228:1046 TCP TTL:64 TOS:0x10 ID:34623 IpLen:20 DgmLen:120 DF*
- ****AP*** Seq: 0xD0C5F09D Ack: 0x5BA57B6E Win: 0xF53C TcpLen: 20*
- =+

IDS – Snort

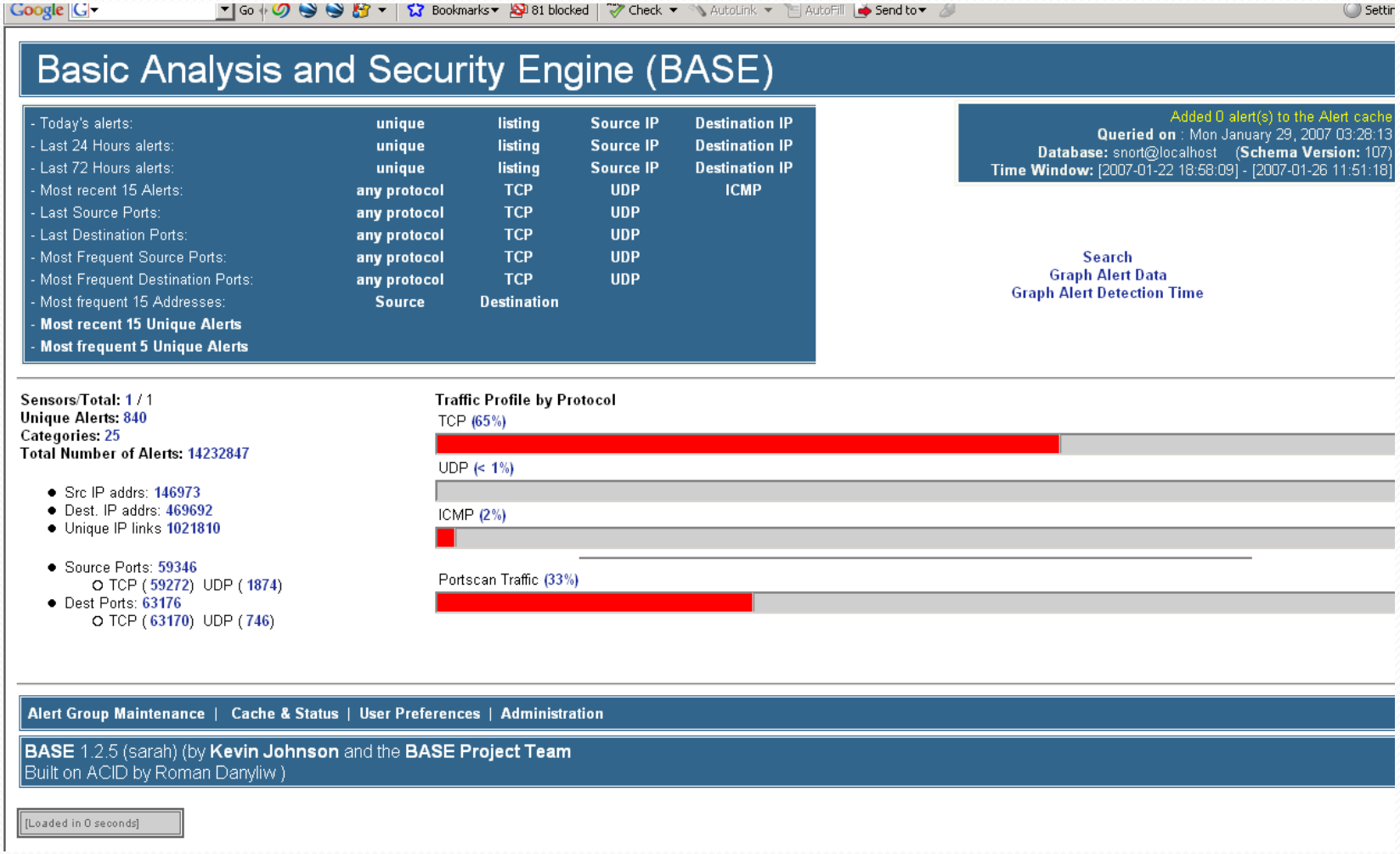
- ***Sistemi kullanmadan önce snort.conf dosyasını ayarlamak gerekmektedir;***
- *# vi snort.conf*
- *var HOME_NET [10.1.1.0/24,192.168.1.0/24]*
-
- ***Genelde varsayılan tanımlar başlangıç için yeterli olmaktadır. Daha iyi bir ayarlama için tavsiyemiz her zamanki gibi kullanım klavuzunu (http://www.snort.org/docs/) okumak olacaktır;***
- ***Günlüğü nasıl tutacağınıza karar vermeniz gerekecektir. Eskiden beri kullanılan en kolay yollardan biri;***
- *output alert_fast: snort-alert-fast.log*
- ***Veya;***
- *output database: log, mysql, user=root password=test dbname=db host=localhost*
- ***Tabii veritabani uygulaması için en başta uygulamayı derlerken (**--with-mysql**) opsiyonunu kullanmak gerekir. Daha sonra MYSQL kurulu cihaz üzerinde;***
- *# mysql SNORT -p < ./schemas/create_mysql*
- ***Komutu uygulanır. Bu komut sayesinde snort'un kullanacağı tablolar oluşturulur. "**create_mysql**" ve diğer dosyalar snort'un kaynak dosyalarının içerisindedir. Oluşturulan snort.conf dosyasındaki iz dosyaları irdelenmeli ve daha önce de indirdiğimiz dosyalarda göz önünde bulundurulmalıdır.***
- *# snort -T -c /usr/local/etc/snort/snort.conf*
- ***Komutu ile de oluşturulan dosyanın test edilmesi sağlanır. Son olarak;***
- *# snort -Dd -c /usr/local/etc/snort/snort.conf*
- ***Komutu ile snort'un arka planda çalışması sağlanır. Günlük bilgileri "**/var/log/snort**" görmeye başlayabilirsiniz. Tabii eğer veritabanı opsiyonu kullanmadı iseniz.***

IDS – Snort

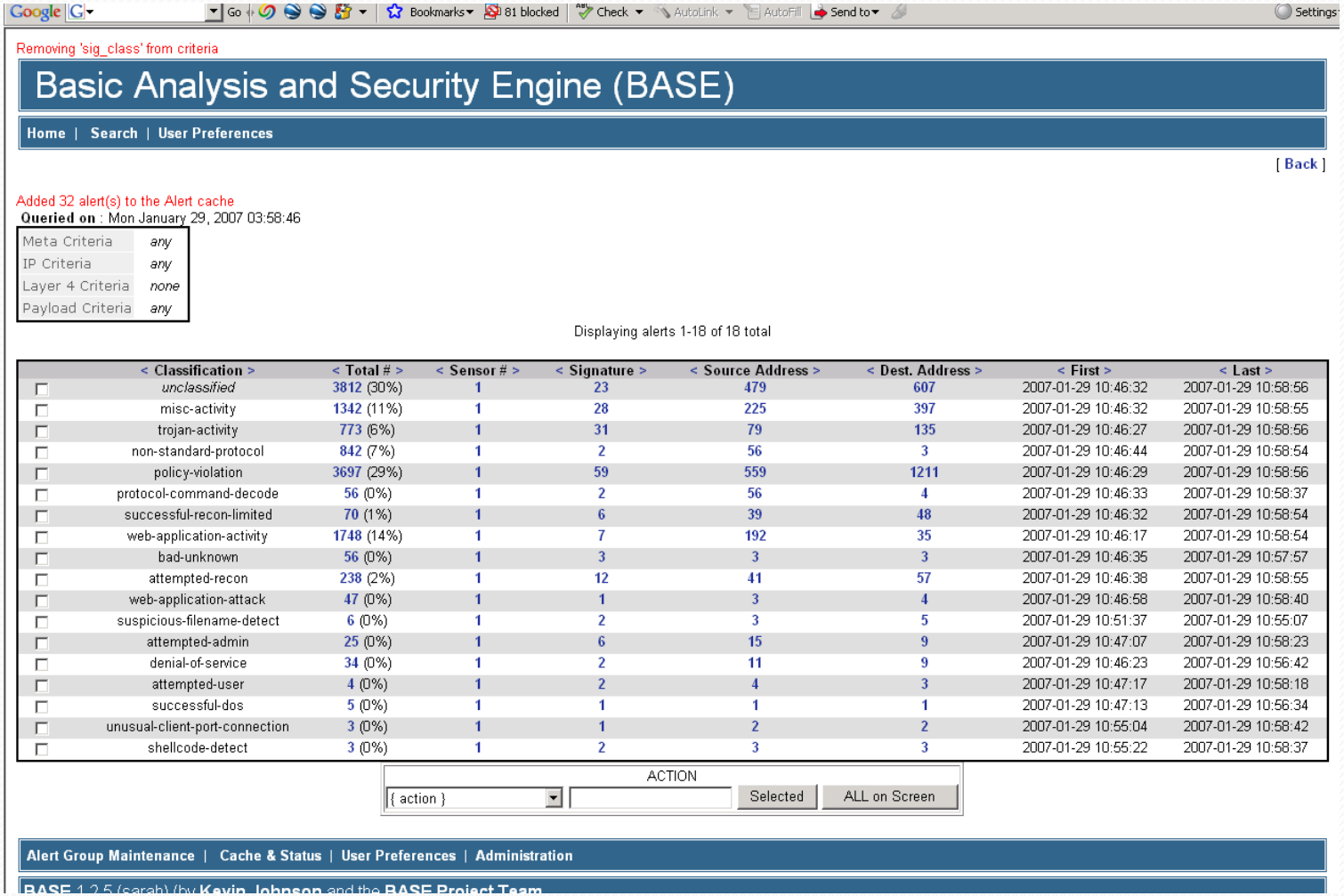
- Burada önemli olan nokta kurulumun tüm olarak anlatılmadığı ve pek çok ara basamağın atlandığıdır. Mesela "*/var/log/snort*" kütüğü olmadığı için alınacak hata mesajı için bu kütük oluşturulmalıdır (*mkdir –p /var/log/snort*). Aynı şekilde kural dizini olmadığı hatasını aldığınız zaman;
- *# mkdir –p /usr/local/snort/rules*
- *# tar zxf snortrules-snapshot-CURRENT.tar.gz*
- *# tar zxf Community-Rules-CURRENT.tar.gz*
- *# tar zxf bleeding.rules.tar.gz*
- *# cp rules/* /usr/local/snort/rules/*

- Böylece tüm kural silsilesi tek bir kütük içerisine yerleştirilmiş olacaktır. Kuralların otomatik güncellemesi için http://oinkmaster.sourceforge.net/ adresinden faydalanabilirsiniz.
  - Kurulumu çok basit.
  - Perl betiklerinden oluşmaktadır.
  - Community-Rules.tar.gz → Community-Rules-CURRENT.tar.gz

IDS – BASE


Google
Go
Bookmarks
81 blocked
Check
AutoLink
AutoFill
Send to
Basic Analysis and Security Engine (BASE)
- Today's alerts: unique listing Source IP Destination IP
- Last 24 Hours alerts: unique listing Source IP Destination IP
- Last 72 Hours alerts: unique listing Source IP Destination IP
- Most recent 15 Alerts: any protocol TCP UDP ICMP
- Last Source Ports: any protocol TCP UDP
- Last Destination Ports: any protocol TCP UDP
- Most Frequent Source Ports: any protocol TCP UDP
- Most Frequent Destination Ports: any protocol TCP UDP
- Most frequent 15 Addresses: Source Destination
- Most recent 15 Unique Alerts
- Most frequent 5 Unique Alerts
Added 0 alert(s) to the Alert cache
Queried on : Mon January 29, 2007 03:28:13
Database: snort@localhost (Schema Version: 107)
Time Window: [2007-01-22 18:58:09] - [2007-01-26 11:51:18]
Search
Graph Alert Data
Graph Alert Detection Time
Sensors/Total: 1 / 1
Unique Alerts: 840
Categories: 25
Total Number of Alerts: 14232847
Src IP addrs: 146973
Dest. IP addrs: 469692
Unique IP links 1021810
Source Ports: 59346
TCP (59272) UDP (1874)
Dest Ports: 63176
TCP (63170) UDP (746)
Traffic Profile by Protocol
TCP (65%)
UDP (< 1%)
ICMP (2%)
Portscan Traffic (33%)
Alert Group Maintenance | Cache & Status | User Preferences | Administration
BASE 1.2.5 (sarah) (by Kevin Johnson and the BASE Project Team
Built on ACID by Roman Danyliw)
[Loaded in 0 seconds]

IDS – BASE



Google | Go | Bookmarks | 81 blocked | Check | AutoLink | AutoFill | Send to | Settings

Removing 'sig_class' from criteria

Basic Analysis and Security Engine (BASE)

Home | Search | User Preferences

[Back]

Added 32 alert(s) to the Alert cache

Queried on : Mon January 29, 2007 03:58:46

Meta Criteria	*any*
IP Criteria	*any*
Layer 4 Criteria	*none*
Payload Criteria	*any*

Displaying alerts 1-18 of 18 total

< Classification >	< Total # >	< Sensor # >	< Signature >	< Source Address >	< Dest. Address >	< First >	< Last >
unclassified	3812 (30%)	1	23	479	607	2007-01-29 10:46:32	2007-01-29 10:58:56
misc-activity	1342 (11%)	1	28	225	397	2007-01-29 10:46:32	2007-01-29 10:58:55
trojan-activity	773 (6%)	1	31	79	135	2007-01-29 10:46:27	2007-01-29 10:58:56
non-standard-protocol	842 (7%)	1	2	56	3	2007-01-29 10:46:44	2007-01-29 10:58:54
policy-violation	3697 (29%)	1	59	559	1211	2007-01-29 10:46:29	2007-01-29 10:58:56
protocol-command-decode	56 (0%)	1	2	56	4	2007-01-29 10:46:33	2007-01-29 10:58:37
successful-recon-limited	70 (1%)	1	6	39	48	2007-01-29 10:46:32	2007-01-29 10:58:54
web-application-activity	1748 (14%)	1	7	192	35	2007-01-29 10:46:17	2007-01-29 10:58:54
bad-unknown	56 (0%)	1	3	3	3	2007-01-29 10:46:35	2007-01-29 10:57:57
attempted-recon	238 (2%)	1	12	41	57	2007-01-29 10:46:38	2007-01-29 10:58:55
web-application-attack	47 (0%)	1	1	3	4	2007-01-29 10:46:58	2007-01-29 10:58:40
suspicious-filename-detect	6 (0%)	1	2	3	5	2007-01-29 10:51:37	2007-01-29 10:55:07
attempted-admin	25 (0%)	1	6	15	9	2007-01-29 10:47:07	2007-01-29 10:58:23
denial-of-service	34 (0%)	1	2	11	9	2007-01-29 10:46:23	2007-01-29 10:56:42
attempted-user	4 (0%)	1	2	4	3	2007-01-29 10:47:17	2007-01-29 10:58:18
successful-dos	5 (0%)	1	1	1	1	2007-01-29 10:47:13	2007-01-29 10:56:34
unusual-client-port-connection	3 (0%)	1	1	2	2	2007-01-29 10:55:04	2007-01-29 10:58:42
shellcode-detect	3 (0%)	1	2	3	3	2007-01-29 10:55:22	2007-01-29 10:58:37

ACTION

{ action } | Selected | ALL on Screen

Alert Group Maintenance | Cache & Status | User Preferences | Administration

BASE 1.2.5 (sarah) (by Kevin Johnson and the BASE Project Team

RRDTool ve LOG Tutma

- RRDTool esasen bir veritabanı uygulaması.
  - http://oss.oetiker.ch/rrdtool
  - Veri depolamak için ideal bir araç.
  - El ile kurulabilmekle beraber;
    - *aptitude install rrdtool*
- *CACTI*
  - *RRDTool kullanılarak oluşturulmuş bir sistem.*
  - *Kurulumu ve işletimi kolay.*
  - *Hızlı veri toplama ve grafik imkanı.*

RRDTool – Örnek

- İlk önce veri tabanı oluşturalım.

```
#!/bin/sh
cd /var/log/rrdtool/
if [ ! -f bandwith_eth0.rrd ]; then
rrdtool create bandwith_eth0.rrd --start N \
        DS:inByte:COUNTER:600:U:U \
        DS:outByte:COUNTER:600:U:U \
        DS:inPKT:COUNTER:600:U:U \
        DS:outPKT:COUNTER:600:U:U \
        DS:inDrop:COUNTER:600:U:U \
        DS:outDrop:COUNTER:600:U:U \
        RRA:AVERAGE:0.5:1:105120 RRA:MAX:0.5:6:35040
fi

if [ ! -f bandwith_eth1.rrd ]; then
rrdtool create bandwith_eth1.rrd --start N \
        DS:inByte:COUNTER:600:U:U \
        DS:outByte:COUNTER:600:U:U \
        DS:inPKT:COUNTER:600:U:U \
        DS:outPKT:COUNTER:600:U:U \
        DS:inDrop:COUNTER:600:U:U \
        DS:outDrop:COUNTER:600:U:U \
        RRA:AVERAGE:0.5:1:105120 RRA:MAX:0.5:6:35040
fi

if [ ! -f meminfo.rrd ]; then
rrdtool create meminfo.rrd --step 300 --start N \
                DS:MemTotal:GAUGE:600:0:U \
                DS:MemFree:GAUGE:600:0:U \
                DS:Buffers:GAUGE:600:0:U \
                DS:Cached:GAUGE:600:U:U \
                DS:SwapCached:GAUGE:600:U:U \
                DS:Active:GAUGE:600:U:U \
                DS:Inactive:GAUGE:600:U:U \
                DS:HighTotal:GAUGE:600:U:U \
                DS:HighFree:GAUGE:600:U:U \
                DS:LowTotal:GAUGE:600:U:U \
                DS:LowFree:GAUGE:600:U:U \
                DS:SwapTotal:GAUGE:600:U:U \
                DS:SwapFree:GAUGE:600:0:U \
                DS:Dirty:GAUGE:600:0:100 \
                DS:Writeback:GAUGE:600:0:100 \
                DS:Mapped:GAUGE:600:0:100 \
                DS:Slab:GAUGE:600:0:100 \
                DS:CommitLimit:GAUGE:600:0:100 \
                DS:Committed_AS:GAUGE:600:0:100 \
                DS:PageTables:GAUGE:600:0:100 \
                DS:VmallocTotal:GAUGE:600:0:100 \
                DS:VmallocUsed:GAUGE:600:0:100 \
                DS:VmallocChunk:GAUGE:600:0:100 \
                RRA:AVERAGE:0.5:2:2000

fi

if [ ! -f loadavg.rrd ]; then
rrdtool create loadavg.rrd --step 60 --start N \
                DS:Load1Min:GAUGE:60:0:U \
                DS:Load5Min:GAUGE:60:0:U \
                DS:Load15Min:GAUGE:60:0:U \
                RRA:AVERAGE:0.5:1:86400
fi
cd –
```

RRDTool – Örnek

- Arayüz bilgileri için:

```
#!/usr/bin/perl -w

$RRDUPDATE="/usr/bin/rrdupdate";
$DBPATH="/var/log/rrdtool";

$values=(qx!/bin/cat /proc/net/dev!);
@values=split(/\n/,$values);

# Eth0 icin;
@interface_eth0=split(/\W+/,$values[3]);
$inByte="$interface_eth0[2]";
$inPKT="$interface_eth0[3]";
$inDrop="$interface_eth0[5]";
$outByte="$interface_eth0[10]";
$outPKT="$interface_eth0[11]";
$outDrop="$interface_eth0[12]";
$tmp=(qx!$RRDUPDATE $DBPATH/bandwith_eth0.rrd
      N:$inByte:$outByte:$inPKT:$outPKT:$inDrop:$outDrop
!);

# Eth1 icin;
@interface_eth1=split(/\W+/,$values[4]);
$inByte="$interface_eth1[2]";
$inPKT="$interface_eth1[3]";
$inDrop="$interface_eth1[5]";
$outByte="$interface_eth1[10]";
$outPKT="$interface_eth1[11]";
$outDrop="$interface_eth1[12]";
$tmp=(qx!$RRDUPDATE $DBPATH/bandwith_eth1.rrd
      N:$inByte:$outByte:$inPKT:$outPKT:$inDrop:$outDrop
!);
```

- CPU Yük Durumu için:

```
#!/usr/bin/perl  -w
$RRDUPDATE="/usr/bin/rrdupdate";
$DBPATH="/var/log/rrdtool";
$values=(qx!/bin/cat /proc/loadavg!);
@value=split(/\ +/,$values);
$putit="N:" . $value[0] . ":" . $value[1] . ":" . $value[2];
$tmp=(qx!$RRDUPDATE $DBPATH/loadavg.rrd $putit !);
```

- Hafıza bilgileri ile ilgili genel istatistiksel bilgiler için:

```
#!/usr/bin/perl -w
$RRDUPDATE="/usr/bin/rrdupdate";
$DBPATH="/var/log/rrdtool";
$values=(qx!/bin/cat /proc/meminfo!);
@values=split(/\n/,$values);
$putit = "N" ;
foreach (@values) {
      @value=split(/\W+/,$_);
      $putit=$putit . ":" . "$value[1]";
}
$tmp=(qx!$RRDUPDATE $DBPATH/meminfo.rrd $putit !);
```

RRDTool – Örnek

- Grafik çizdirmek için:

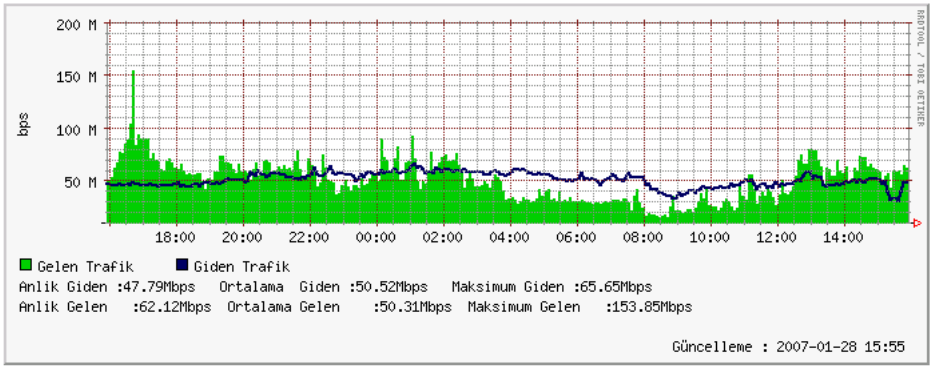
```
#!/bin/sh

RRDTOOL="/usr/bin/rrdtool graph "
GRAPHS="/var/log/rrdtool/graph/new"

date=`date +"%F %R"`
cd /var/log/rrdtool/

$RRDTOOL $GRAPHS/kampus-day.png --start -1d -w 600 -h 150 -v bps \
      "DEF:in=bandwith_eth0.rrd:inByte:AVERAGE" "DEF:out=bandwith_eth0.rrd:outByte:AVERAGE" \
      'CDEF:bin=in,8,*'       'CDEF:bout=out,8,*' \
      'AREA:bout#00CC00:Gelen Trafik    ' 'LINE2:bin#000066:Giden Trafik:STACK \l' \
      "COMMENT:\n" \
      'GPRINT:bin:LAST:Anlik Giden \:%3.2lf%sbps ' 'GPRINT:bin:AVERAGE:Ortalama  Giden \:%3.2lf%sbps '
    'GPRINT:bin:MAX:Maksimum Giden \:%3.2lf%sbps \l' \
      'GPRINT:bout:LAST:Anlik Gelen    \:%3.2lf%sbps' 'GPRINT:bout:AVERAGE:Ortalama Gelen     \:%3.2lf%sbps'
    'GPRINT:bout:MAX:Maksimum Gelen    \:%3.2lf%sbps \l'  \
      "COMMENT:\n" \
      "COMMENT: Güncelleme : $date \r“
```

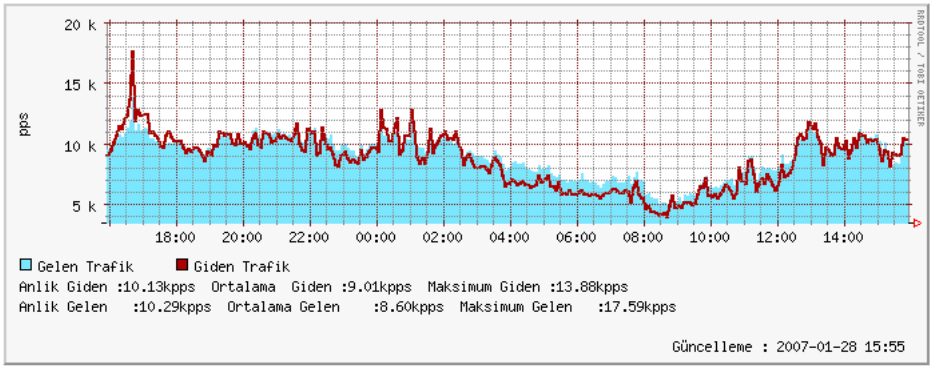
- *removespikes.pl*
- *Bazı versiyonlar arasında farklılık vardır.*

RRDTool – Örnek

Kampüs Dışı Toplam Kullanım İstatistikleri

Günlük kullanım istatistikleri:

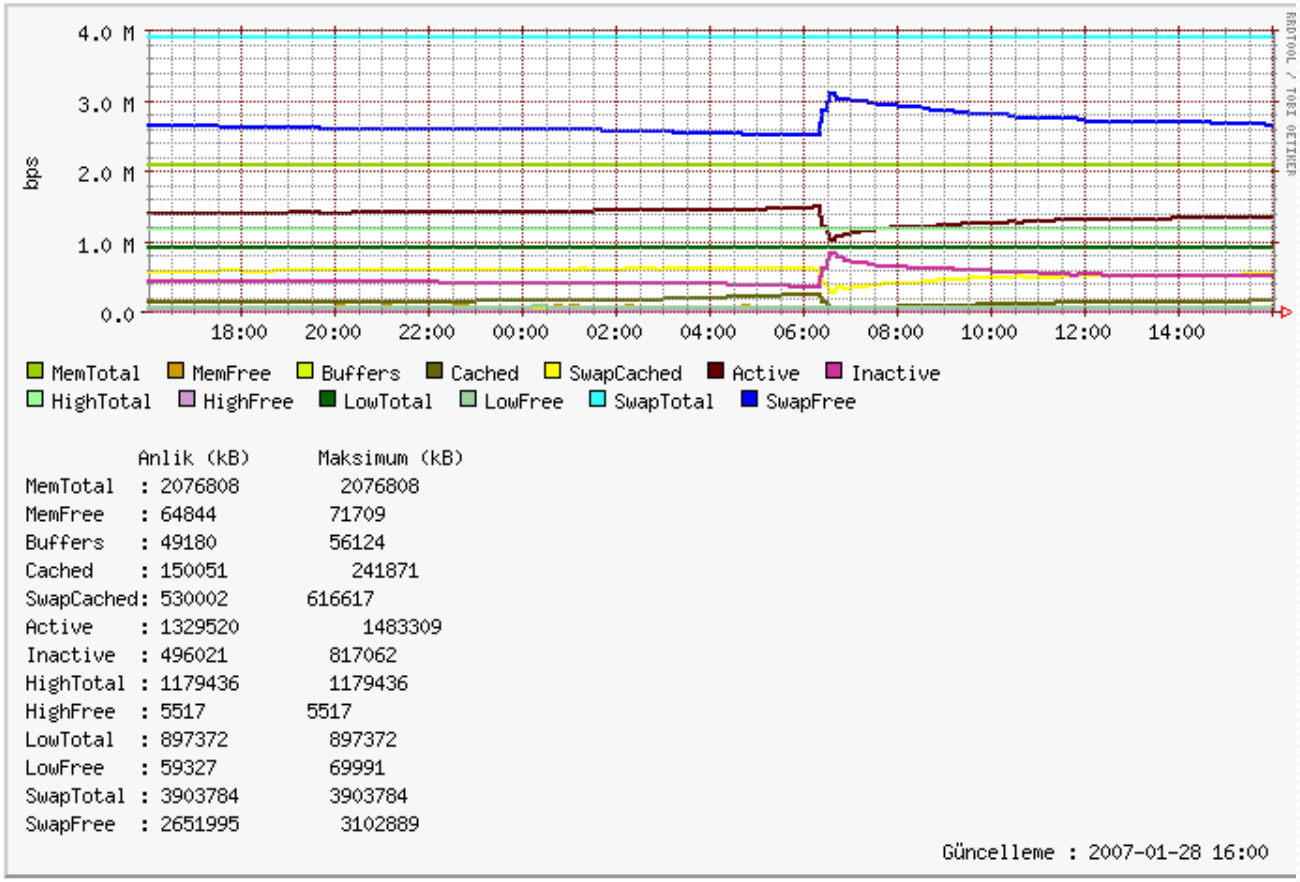




Haftalık kullanım istatistikleri:

RRDTool – Örnek

Günlük kullanım istatistikleri:

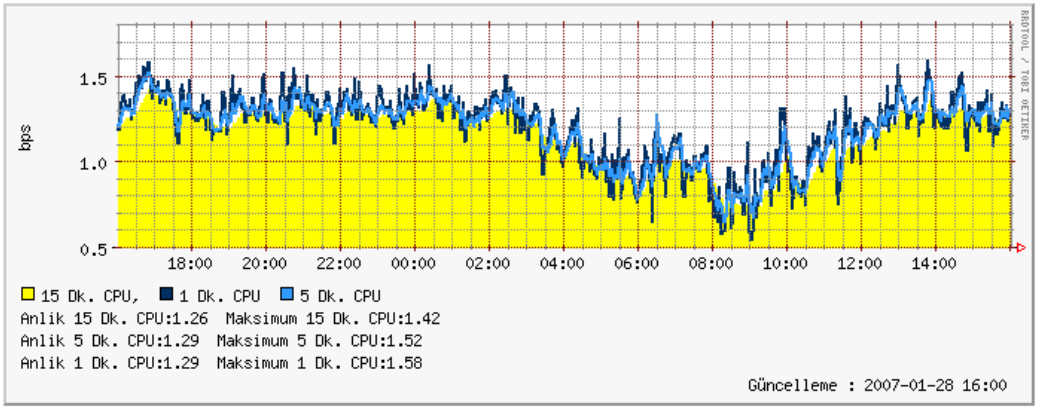


	Anlik (kB)	Maksimum (kB)
MemTotal	: 2076808	2076808
MemFree	: 64844	71709
Buffers	: 49180	56124
Cached	: 150051	241871
SwapCached	: 530002	616617
Active	: 1329520	1483309
Inactive	: 496021	817062
HighTotal	: 1179436	1179436
HighFree	: 5517	5517
LowTotal	: 897372	897372
LowFree	: 59327	69991
SwapTotal	: 3903784	3903784
SwapFree	: 2651995	3102889

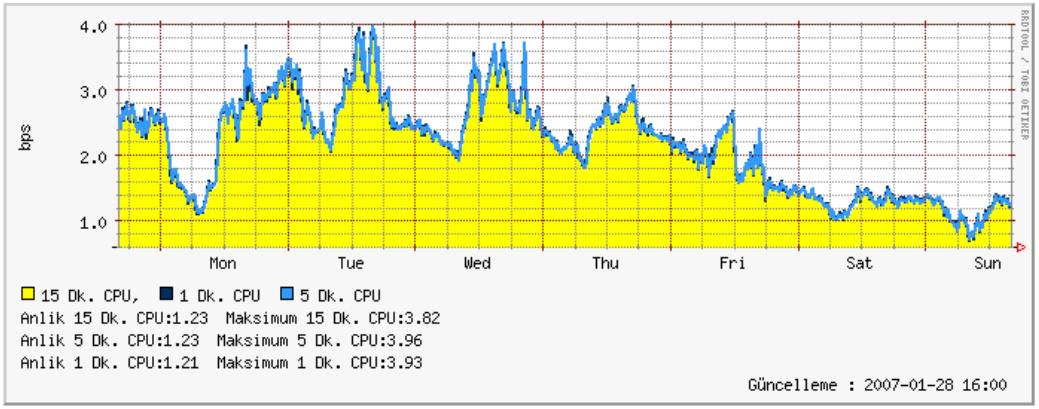
Güncelleme : 2007-01-28 16:00

RRDTool – Örnek

Günlük kullanım istatistikleri:



Haftalık kullanım istatistikleri:



Sistem Ayarları

- Eğer çekirdeği derlerken yönlendirici olarak seçmedi iseniz:

  # sysctl -w net.ipv4.ip_forward=1

- Her açılışta aynı komutu yazmaktansa "*sysctl.conf*" dosyasına ekleme yapabilirsiniz.
- Eğer birden fazla İnternet bağlantınız var ise:

  # sysctl –w net.ipv4.conf.all.rp_filter=0

- Şu ayarlar genelde iyi çalışır.
- *# cat sysctl.conf*

  net/ipv4/ip_conntrack_max=1310720
  net/ipv4/tcp_sack=0
  net/ipv4/tcp_timestamps=0
  net/core/rmem_max=16777216
  net/core/wmem_max=16777216
  net/ipv4/tcp_rmem = 4096 87380 16777216
  net/ipv4/tcp_wmem = 4096 65536 16777216
  net/core/netdev_max_backlog=300000
  net/ipv4/tcp_fin_timeout=15
  net/ipv4/netfilter/ip_conntrack_tcp_timeout_fin_wait=15
  net/ipv4/conf/default/accept_source_route=0
  net/ipv4/conf/default/accept_redirects=0
  net/ipv4/conf/all/accept_source_route=0
  net/ipv4/conf/all/accept_redirects=0

- Önemli olan nokta her sistem için farklı ayarlamalar olduğudur.

Sistem Ayarları

- Conntrack modülü parametrelerine dikkat.
  - Bu parametreler RAM hesabına göre yapılmaktadır.
  - hashsize ile performans arttırılabilir.
    - **modprobe.conf** dosyasına

      options ip_conntrack hashsize=163840
- Conntrack modülünün bir kere yüklenmesi tüm bağlantıların izlenmesine neden olur.

  # cat /proc/net/ip_conntrack
- Bu modül sistemin yavaşlamasına neden olur.
- Bazı durumlarda DDoS'a açık hale getirir.

Sistem Ayarları

Unutmayın ki her sistemin kendine özgü yapısı vardır.

Kurulan sistem en başta sorunlara sahip olacaktır.

Zamanla bu sorunların üstesinden geleceğinizi göreceksiniz.

Sistem denemelerinizi canlı ağa aktarmadan önce küçükten başlamanız önerilir.

DİKKAT

Kullanıcılarınız ve özellikle yöneticileriniz size sinirlenecektir.

Iptables - Örnek

eth0 : İç ağ 10.0.0.1
eth1 : dış ağ x.y.z
Spoofing engelleme ve loglama
iptables -A FORWARD -s 10.0.0.0/255.255.0.0 -i ! eth0 -j LOG --log-prefix "Spoofing ..."
iptables -A FORWARD -s 10.0.0.0/255.255.0.0 -i ! eth0 -j DROP
iptables -A FORWARD -s ! 10.0.0.0/255.255.0.0 -i eth0 -j LOG --log-prefix “Iceriden Spoofing ..."
iptables -A FORWARD -s ! 10.0.0.0/255.255.0.0 -i eth0 -j DROP
Adında anlaşılacağı üzere geçersiz paketleri düşür.
iptables -A FORWARD -i eth0 -m state --state INVALID -j DROP
İçeriden dışarıya izin ver. Dışarıdan içeriye gelenleri durdur.
iptables -A FORWARD -i eth0 -m state --state NEW,RELATED,ESTABLISHED –s 10.0.0.0/255.255.0.0 –j ACCEPT
iptables -A FORWARD -o eth0 -m state –state RELATED,ESTABLISHED –d 10.0.0.0/255.255.0.0 –j ACCEPT
iptables -A FORWARD -o eth0 -d 10.0.0.0/255.255.0.0 –j DROP
ICMP – Dikkat edileceği gibi tüm ICMP gidişine izin verilmiştir.
iptables -A FORWARD -o eth0 -p icmp -m icmp --icmp-type 8 -j ACCEPT
iptables -A FORWARD -o eth0 -p icmp -m icmp --icmp-type 0 -j ACCEPT
iptables -A FORWARD -o eth0 -p icmp -m icmp --icmp-type 11 -j ACCEPT
iptables -A FORWARD -o eth0 -p icmp -m icmp --icmp-type 3/4 -j ACCEPT
iptables -A FORWARD -o eth0 -p icmp -j DROP

Iptables - Örnek

eth0 : İç ağ 10.0.0.1

eth1 : dış ağ x.y.z

ipset let kullanım.

```
ipset -N Karaliste iphash --hashsize 1024 --probes 8 --resize 50
ipset –A Karaliste 192.168.0.1
ipset -N KaralisteAg nethash --hashsize 1024 --probes 4 --resize
      50
ipset -A KaralisteAg 127.0.0.0/8
ipset -A KaralisteAg 172.16.0.0/12
ipset -A KaralisteAg 192.168.0.0/16
iptables  -A FORWARD -i eth1 -m set --set Karaliste src –j DROP
iptables -A FORWARD  -m set --set KaralisteAg src –j DROP
```

Iptables'ın "connlimit" ve "hashlimit" fonksiyonu;

```
connlimit v1.3.7 options:
[!] --connlimit-above n        match if the number of existing tcp connections is (not) above n
 --connlimit-mask n            group hosts using mask


hashlimit v1.3.7 options:
--hashlimit <avg>              max average match rate
                               [Packets per second unless followed by
                               /sec /minute /hour /day postfixes]
--hashlimit-mode <mode>        mode is a comma-separated list of
                               dstip,srcip,dstport,srcport
--hashlimit-name <name>        name for /proc/net/ipt_hashlimit/
[--hashlimit-burst <num>]      number to match in a burst, default 5
[--hashlimit-htable-size <num>] number of hashtable buckets
[--hashlimit-htable-max <num>]  number of hashtable entries
[--hashlimit-htable-gcinterval] interval between garbage collection runs
[--hashlimit-htable-expire]    after which time are idle entries expired?
```

```
iptables -A FORWARD -o eth0 -p icmp -m hashlimit  \
      --hashlimit 2/min --hashlimit-burst 2 \
      --hashlimit-mode srcip --hashlimit-name ICMP \
      -m icmp --icmp-type 8 -j ACCEPT
iptables -A INPUT -p tcp --dport 80 -m connlimit  \
      --connlimit-above 3 –j REJECT --reject-with tcp-reset
```

Özellikle son satır DDoS saldırılarında yararlı olabilir. Tabii hashlimit modülüde gayet başarılı.

TEŞEKKÜR EDERİZ

ccnet@metu.edu.tr