

Özgür Yazılımlarla 5651'e Uygun Kayıt Tutmak

Yrd. Doç. Dr. Hüseyin YÜCE

Özgür Yazılım ve Linux Günleri- 1-2 Nisan 2011



- » 5651 No'lu Yasa ve ilgili Yönetmelikler
- » Yasa ve yönetmeliklerde üniversitenin yeri
- » Üniversitenin yükümlülükleri
- » IP Yönetim Sistemi
- » Kullanıcı Tespiti
- » Loglama
- » Log imzalama

İçerik



5651?

- » 4/5/2007 Tarihli ve 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

İlgili Yönetmelikler:

- » 24/10/2007 tarihli ve 26680 sayılı Resmi Gazetede yayımlanan Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik
- » 01/11/2007 tarih ve 26687 sayılı Resmi Gazetede yayımlanan İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik
- » 30/11/2007 tarihli 26716 sayılı Resmi Gazetede yayımlanan İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik



- » **Erişim sağlayıcı:** Kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişileri,
- » **İçerik sağlayıcı:** İnternet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişileri,
- » **Trafik bilgisi:** İnternet ortamında gerçekleştirilen her türlü erişime ilişkin olarak taraflar, zaman, süre, yararlanılan hizmetin türü, aktarılan veri miktarı ve bağlantı noktaları gibi değerleri,

5651 - Tanımlar



- » **Faaliyet Belgesi:** Erişim sağlayıcı veya yer sağlayıcı olarak faaliyette bulunabilmek için Kurum tarafından verilen 5651 sayılı Kanun kapsamındaki yetkilendirmeyi içeren belgeyi,
- » **Ticari amaçla internet toplu kullanım sağlayıcı:** İnternet salonu ve benzeri umuma açık yerlerde belirli bir ücret karşılığı internet toplu kullanım sağlayıcılığı hizmeti veren veya bununla beraber bilgisayarlarda bilgi ve beceri artırıcı veya zekâ geliştirici nitelikteki oyunların oynatılmasına imkân sağlayanı,
- » **Yer sağlayıcı trafik bilgisi:** İnternet ortamındaki her türlü yer sağlamaya ilişkin olarak; kaynak IP adresi, hedef IP adresi, bağlantı tarih-saat bilgisi, istenen sayfa adresi, işlem bilgisi (GET, POST komut detayları) ve sonuç bilgisi gibi bilgileri,

26680-Tanımlar



» Erişim sağlayıcının yükümlülükleri;

- Erişim sağlayıcı trafik bilgisini bir yıl saklamakla, bu bilgilerin doğruluğunu, bütünlüğünü oluşturan verilerin dosya bütünlük değerlerini (hash) zaman damgası ile birlikte muhafaza etmek ve gizliliğini temin etmekle,

» Yer sağlayıcının yükümlülükleri;

- Faaliyet Belgesi alınacak.
- Yer sağlayıcı trafik bilgisini altı ay saklamakla, bu bilgilerin doğruluğunu, bütünlüğünü oluşturan verilerin dosya bütünlük değerlerini (hash) zaman damgası ile birlikte saklamak ve gizliliğini temin etmekle yükümlüdür

26680-Yükümlülükler >

- » **Erişim sağlayıcı:** İnternet toplu kullanım sağlayıcılarına ve abone olan kullanıcılarına internet ortamına erişim olanağı sağlayan işletmeciler ile gerçek veya tüzel kişileri,
- » **İnternet toplu kullanım sağlayıcı:** Kişilere belli bir yerde ve belli bir süre internet ortamı kullanım olanağı sağlayan gerçek ve tüzel kişileri,
- » **İç IP Dağıtım Logları:** Kendi iç ağlarında dağıtılan IP adres bilgilerini, kullanıma başlama ve bitiş tarih ve saatini ve bu IP adreslerini kullanan bilgisayarların tekil ağ cihaz numarasını (MAC adresi) gösteren bilgileri,

26687-Tanımlar



» **İnternet toplu kullanım sağlayıcı;**

- Konusu suç oluşturan içeriklere erişimi önleyici tedbirleri almak.
- İç IP Dağıtım Loglarını elektronik ortamda kendi sistemlerine kaydetmek

» **Ticari amaçla internet toplu kullanım sağlayıcı;**

- » İç IP Dağıtım Loglarını elektronik ortamda kendi sistemlerine kaydetmek.
- » Başkanlık tarafından verilen yazılım ile, (d) bendi gereğince kaydedilen bilgileri ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini teyit eden değeri kendi sistemlerine günlük olarak kaydetmek ve bu verileri bir yıl süre ile saklamak.

26687-Yükümlülükler >

- » **Dosya bütünlük değeri:** Bir bilgisayar dosyasının içindeki bütün verilerin matematiksel bir işlemde geçirilmesi sonucu elde edilen ve dosyanın içerisindeki verilerde bir değişiklik yapıp yapılmadığını kontrol için kullanılan dosyanın özünü belirten değeri,
- » **Erişim sağlayıcı trafik bilgisi:** İnternet ortamında yapılan her türlü erişime ilişkin olarak abonenin adı, kimlik bilgileri, adı ve soyadı, adresi, telefon numarası, sisteme bağlantı tarih ve saat bilgisi, sistemden çıkış tarih ve saat bilgisi, ilgili bağlantı için verilen IP adresi ve bağlantı noktaları gibi bilgileri,
- » **Vekil sunucu trafik bilgisi:** İnternet ortamında erişim sağlayıcı tarafından kullanılan vekil sunucu hizmetine ilişkin talebi yapan kaynak IP adresi ve port numarası, erişim talep edilen hedef IP adresi ve port numarası, protokol tipi, URL adresi, bağlantı tarih ve saati ile bağlantı kesilme tarih ve saati bilgisi gibi bilgileri,

26716-Tanımlar



» Yer sağlayıcı;

- Yer sağlayıcı trafik bilgisini altı ay saklamakla, bu bilgilerin doğruluğunu, bütünlüğünü oluşturan verilerin dosya bütünlük değerlerini zaman damgası ile birlikte saklamak ve gizliliğini temin etmekle

» Erişim sağlayıcı;

- Erişim sağlayıcı trafik bilgisini bir yıl saklamakla, bu bilgilerin doğruluğunu, bütünlüğünü oluşturan verilerin dosya bütünlük değerlerini zaman damgası ile birlikte muhafaza etmek ve gizliliğini temin etmekle
- Kullanıcılarına vekil sunucu hizmeti sunuyor ise; vekil sunucu trafik bilgisini bir yıl saklamakla, bu bilgilerin doğruluğunu, bütünlüğünü oluşturan verilerin dosya bütünlük değerlerini zaman damgası ile birlikte muhafaza etmek ve gizliliğini temin etmekle


26716-Yükümlülükler >

- ❑ 5651 sayılı kanun ve bu kanuna bağlı yönetmelikler incelendiğinde kamu kurumları;
- Faaliyet Belgesi Almak
- Trafik Bilgisini Saklamak
- Konusu suç oluşturan içeriklere erişimi önleyici tedbirleri almak.
- İç IP Dağıtım Loglarını Tutmak
-

'e Göre



PHP DHCP Admin

**Marmara Üniversitesi**

[Anasayfa](#)
[IP Tahsisi](#)
[Tercihler](#)
[DHCP Yinele](#)
[Oturumu Kapat](#)

Users: 11 online
Load Time: 1.787ms

DHCP Yonetim Paneli

Manage Static Hosts

Bilgisarları Yönet

Buradan bilgisayarlara sabit ip atayabilirsiniz.

S

Bilgisayar Ekle/Güncelle/Sil

** Tüm Alanlar doldurmak zorunludur.

T.C. Kimlik:	<input type="text"/>	* 12345678910
Adı:	<input type="text"/>	* Alican
Soyadı:	<input type="text"/>	* Çoksever
Email:	<input type="text"/>	* alican@marmara.edu.tr
Bilgisayar Adı:	<input type="text"/>	* Sadece inglizce karakter kullanınız.
IP Adres:	<input type="text"/>	* 192.168.0.21
MAC Adres:	<input type="text"/>	* 00:ef:78:b0:ad:e4
Altağ Seç:	<input type="text" value="rektorlukRealSubnet"/>	* Subnet?
PXE Seç :	No PXE Groups defined	* PXE Group?

[ekle](#) [Güncelle](#) [Sil](#)
[Temizle](#)

Ad	Soyad	HostName	Mac	IP
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

rektorlukRealSubnet

IP Durumu

Toplam IP: 253
Kullanılan IP: 240
Kalan IP: 13

Boş IP Listesi

193.255.166.120
193.255.166.155
193.255.166.156
193.255.166.180
193.255.166.182
193.255.166.184

Statik IP nasıl engellenir?

»Güvenlik özellikleri olan yönetimsel anahtarlama cihazlarında “kaynak doğrulama” özelliği etkinleştirilir:

»sw(config)# ip verify source

»Ancak bu komut dhcp snooping veritabanını kullandığı için, öncesinde dhcp snooping etkinleştirilmelidir.

»sw(config)# ip dhcp snooping

»sw(config)# ip dhcp snooping vlan 12

»Dhcp'ye bakan arayüzde:

»sw(config-if)# ip dhcp snooping trust

»Statik IP verilmesi gerektiği durumlarda aşağıdaki gibi bir komut girişi yapılması gerekir:

»ip source binding 001C.7ECC.98AD vlan 947 193.255.92.125 interface Fa0/22

```
SBMYO#sh ip dhcp snooping binding
```

MacAddress	IpAddress	Lease(sec)	Type	VLAN	Interface
00:01:29:5E:4B:69	10.245.1.27	50060	dhcp-snooping	947	FastEthernet0/5
00:1D:92:21:51:93	10.245.1.27	63882	dhcp-snooping	947	FastEthernet0/17
00:0F:FE:E5:FD:8A	10.245.1.27	68540	dhcp-snooping	246	FastEthernet0/2
00:19:DB:DE:5E:86	10.245.1.27	85470	dhcp-snooping	947	FastEthernet0/4
00:0F:FE:E5:9C:96	10.245.1.9	68810	dhcp-snooping	246	FastEthernet0/1
00:0F:FE:E6:5D:6D	10.245.1.13	54374	dhcp-snooping	246	FastEthernet0/1
00:1C:25:6F:AE:30	193.255.92.125	64016	dhcp-snooping	947	FastEthernet0/26
00:01:80:68:F9:E9	10.245.1.27	64618	dhcp-snooping	947	FastEthernet0/37
00:0F:FE:E6:00:30	10.245.1.5	44557	dhcp-snooping	246	FastEthernet0/1
00:1D:92:21:30:AC	10.245.1.27	75960	dhcp-snooping	947	FastEthernet0/21



Kullanıcı Konum Tespiti - 1

Belirli aralıklarla SNMP ile ARP tablolarını çekmek:

```
# snmpwalk -v 1 192.168.100.42 -c 123pass456 .1.3.6.1.2.1.3.1.1.2
```

```
RFC1213-MIB::atPhysAddress.70.1.10.70.0.1 = Hex-STRING: 00 21 1B 29 B3 C1  
RFC1213-MIB::atPhysAddress.70.1.10.70.0.20 = Hex-STRING: 00 0F FE 1D 67 1C  
RFC1213-MIB::atPhysAddress.75.1.10.75.0.1 = Hex-STRING: 00 21 1B 29 B3 C2  
RFC1213-MIB::atPhysAddress.76.1.10.75.1.1 = Hex-STRING: 00 21 1B 29 B3 C3  
RFC1213-MIB::atPhysAddress.76.1.10.75.1.60 = Hex-STRING: 00 0F FE E6 5F 47  
RFC1213-MIB::atPhysAddress.76.1.10.75.1.102 = Hex-STRING: 00 19 DB C0 A9 A1
```

Ya da DHCP logları:

```
Oct 15 17:41:12 fener dhcpd: DHCPDISCOVER from 00:0f:fe:e6:62:58 (sks-PC) via 10.35.0.1  
Oct 15 17:41:13 fener dhcpd: DHCPOFFER on 10.35.0.45 to 00:0f:fe:e6:62:58 (sks-PC) via 10.35.0.1  
Oct 15 17:41:13 fener dhcpd: DHCPREQUEST for 10.35.0.45 (193.140.143.27) from 00:0f:fe:e6:62:58 (sks-PC) via 10.35.0.1  
Oct 15 17:41:13 fener dhcpd: DHCPACK on 10.35.0.45 to 00:0f:fe:e6:62:58 (sks-PC) via 10.35.0.1  
Oct 15 17:41:13 fener dhcpd: DHCPREQUEST for 10.60.6.108 from 00:0f:fe:e6:67:41 (sezgi-PC) via 10.60.6.1  
Oct 15 17:41:13 fener dhcpd: DHCPACK on 10.60.6.108 to 00:0f:fe:e6:67:41 (sezgi-PC) via 10.60.6.1  
Oct 15 17:41:14 fener dhcpd: DHCPINFORM from 10.75.1.17 via 10.75.1.1  
Oct 15 17:41:14 fener dhcpd: DHCPACK to 10.75.1.17 (00:0f:fe:e6:5f:21) via em0
```

Kullanıcı Konum Tespiti - 2

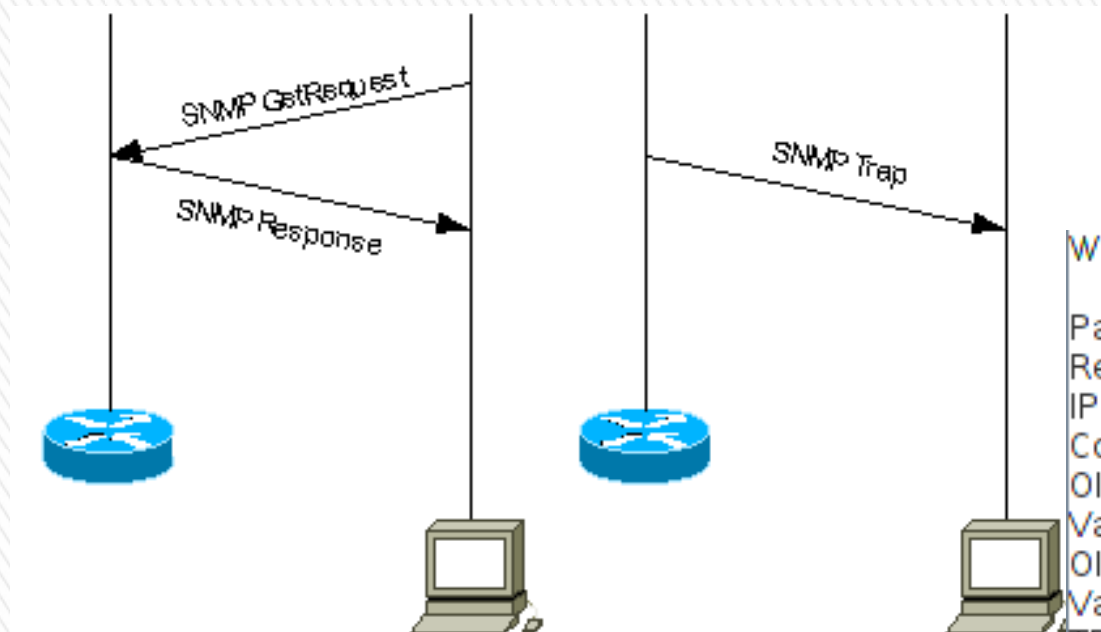
```
NISANTASI_ILETISIM#sh mac address-table
Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
233     000e.8368.45b1    DYNAMIC   Gi0/50
975     000b.6a64.5f25    DYNAMIC   Gi0/42
975     000d.f03c.e309    DYNAMIC   Gi0/46
975     000e.8368.45b1    DYNAMIC   Gi0/50
975     000f.fe76.1aa9    DYNAMIC   Gi0/48
975     000f.fee5.9d46    DYNAMIC   Gi0/3
975     0014.5eb4.7c46    DYNAMIC   Gi0/37
975     0014.857c.08d8    DYNAMIC   Gi0/43
975     001b.fcac.9cb4    DYNAMIC   Gi0/47
975     001d.9200.5e4e    DYNAMIC   Gi0/28
1       000e.8368.4580    DYNAMIC   Gi0/50
```

2) mac-notification snmp trap

Kullanıcı hangi portta hangi s
1) SNMP ile yönetilebilir anahtarlama cihazlarından MAC adres tabloları belirli aralıklarla çekilebilir (5 dakikada 1 gibi...)

```
[tugrul@tugrul-blg macTable]$ cat mactable_20100519152331.txt
VLAN    Port    Fiziksel Adress
233     Gi0/50  00:0E:83:68:45:B1
800     Gi0/50  00:0E:83:68:45:B1
970     Gi0/50  00:0E:83:68:45:B1
970     Gi0/50  00:50:04:C0:66:2D
975     Gi0/42  00:0B:6A:64:5F:25
975     Gi0/46  00:0D:F0:3C:E3:09
975     Gi0/50  00:0E:83:68:45:B1
975     Gi0/48  00:0F:FE:76:1A:A9
975     Gi0/3    00:0F:FE:E5:9D:46
975     Gi0/37  00:14:5E:B4:7C:46
975     Gi0/43  00:14:85:7C:08:D8
975     Gi0/47  00:1B:FC:AC:9C:B4
975     Gi0/28  00:1D:92:00:5E:4E

----- Wed May 19 15:23:31 EEST 2010 -----
```



Waiting for TRAPs or INFORMs...

Packet #1 - SNMP Version 2c TRAP Arrived.
Received: Wed May 19 14:04:33 EEST 2010
IP / Source Port: 192.168.254.2/49929
Community: XXXXXXXXXX
OID #1: 1.3.6.1.2.1.1.3.0
Value #1: 22 days, 0:57:31.93
OID #2: 1.3.6.1.6.3.1.1.4.1.0
Value #2: 1.3.6.1.4.1.9.9.215.2.0.1
TRAP Type: Other
OID #3: 1.3.6.1.4.1.9.9.215.1.1.8.1.2.10
Value #3: 02:00:0b:00:0e:2e:09:d5:a9:00:30:00
OID #4: 1.3.6.1.4.1.9.9.215.1.1.8.1.3.10
Value #4: 190425193

SNMP Trap?



Mac-notification

Rektorluk-l#show mac address-table notification change

.....
History Index 1, Entry Timestamp 174044601, Despatch Timestamp 174044601

MAC Changed Message :

Operation: Added Vlan: 11 MAC Addr: 0014.c134.f3f6 Dot1dBasePort: 38

Operation: Added Vlan: 11 MAC Addr: 000f.fe76.1c5b Dot1dBasePort: 36

Operation: Deleted Vlan: 11 MAC Addr: 0019.bb5c.c5e6 Dot1dBasePort: 31

Rektorluk-l# debug snmp packet

007689: 2w6d: SNMP: Queuing packet to 193.255.92.24

007690: 2w6d: SNMP: V1 Trap, ent cmnMIBNotificationPrefix, addr 192.168.254.2,
gentrap 6, spectrap 1

cmnHistMacChangedMsg.1 =

01 00 0B 00 14 C1 34 F3 F6 00 26 01 00 0B 00 0F

FE 76 1C 5B 00 24 02 00 0B 00 19 BB 5C C5 E6 00

1F 00

cmnHistTimestamp.1 = 174044601

007691: 2w6d: SNMP: Packet sent via UDP to 193.255.92.24



Mac-notification conf

- » Global config:
 - » mac address-table notification change interval 10
 - » mac address-table notification change history-size 10
 - » mac address-table notification change
 - » mac address-table aging-time 300
 - » snmp-server enable traps mac-notification
 - » snmp-server host 192.168.2.24 version 2c 123pass567 mac-notification
- » interface config:
 - » snmp trap mac-notification added
 - » snmp trap mac-notification removed



SNMP Trap'leri Loglamak

- snmptrapd
- snmptt (snmp trap translator)

snmptrapd.conf

- » traphandle default /usr/sbin/snmptt
- » disableAuthorization yes
- » logoption f /var/snmp/snmptrapd.log



snmptrap'leri loglamak

- » `snmptrapd -c /etc/snmp/snmptrapd.conf -M /usr/share/snmp/mibs/`
- » `root@bilisim-desktop:~# tail -f /var/snmp/snmptrapd.log`
- » NET-SNMP version 5.4.2.1
- » 192.168.254.2 [UDP: [193.255.92.24]->[192.168.254.2]:-15607]: Trap , DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (219245061) 25 days, 9:00:50.61, SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-SMI::enterprises.9.9.215.2.0.1, SNMPv2-SMI::enterprises.9.9.215.1.1.8.1.2.7 = Hex-STRING: 02 00 05 00 19 BB 24 46 08 00 07 00 , SNMPv2-SMI::enterprises.9.9.215.1.1.8.1.3.7 = INTEGER: 219245060
- » 192.168.254.2 [UDP: [193.255.92.24]->[192.168.254.2]:-15607]: Trap , DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (219246061) 25 days, 9:01:00.61, SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-SMI::enterprises.9.9.215.2.0.1, SNMPv2-SMI::enterprises.9.9.215.1.1.8.1.2.8 = Hex-STRING: 02 00 0B 00 15 AF 19 7D 1B 00 26 01 00 0B 00 15
- » AF 19 7D 1B 00 26 01 00 0B 00 0E 2E 09 D5 A9 00
- » 30 02 00 0B 00 14 C1 34 F3 F6 00 26 02 00 0B 00
- » 0E 2E 09 22 D0 00 30 00 , SNMPv2-SMI::enterprises.9.9.215.1.1.8.1.3.8 = INTEGER: 219246060



IP Dağıtım Logları - DHCP

dhcpcd.log

```
Oct 15 17:41:12 fener dhcpcd: DHCPDISCOVER from 00:0f:fe:e6:62:58 (sks-PC) via 10.35.0.1
Oct 15 17:41:13 fener dhcpcd: DHCPOFFER on 10.35.0.45 to 00:0f:fe:e6:62:58 (sks-PC) via 10.35.0.1
Oct 15 17:41:13 fener dhcpcd: DHCPREQUEST for 10.35.0.45 (193.140.143.27) from 00:0f:fe:e6:62:58 (sks-PC) via 10.35.0.1
Oct 15 17:41:13 fener dhcpcd: DHCPACK on 10.35.0.45 to 00:0f:fe:e6:62:58 (sks-PC) via 10.35.0.1
Oct 15 17:41:13 fener dhcpcd: DHCPREQUEST for 10.60.6.108 from 00:0f:fe:e6:67:41 (sezgi-PC) via 10.60.6.1
Oct 15 17:41:13 fener dhcpcd: DHCPACK on 10.60.6.108 to 00:0f:fe:e6:67:41 (sezgi-PC) via 10.60.6.1
Oct 15 17:41:14 fener dhcpcd: DHCPINFORM from 10.75.1.17 via 10.75.1.1
Oct 15 17:41:14 fener dhcpcd: DHCPACK to 10.75.1.17 (00:0f:fe:e6:5f:21) via em0
```

dhcpcd.leases

```
lease 10.60.1.10 {
    starts 2 2010/05/18 17:14:04;
    ends 3 2010/05/19 17:14:04;
    cltt 2 2010/05/18 17:14:04;
    binding state active;
    next binding state free;
    hardware ethernet 00:0f:fe:e6:04:46;
    uid "\001\000\017\376\346\004F";
    client-hostname "iibf-PC";
}
```



Log'ların Log sunucusuna gönderilmesi

dhcpcd.conf:

```
log-facility local7;
```

syslog.conf:

```
local7.* @192.168.10.10
```

```
File: messages.log      Line 50 Col 0      5979807 bytes
2010-05-19T00:05:55+03:00 fener dhcpcd: DHCPDISCOVER from 00:16:e0:f3:4f:41 via 193.255.173.129: network 193.255.173.128
2010-05-19T00:05:56+03:00 fener dhcpcd: DHCPDISCOVER from 00:18:6e:41:6a:41 via 193.255.173.129: network 193.255.173.128
2010-05-19T00:05:58+03:00 fener dhcpcd: DHCPDISCOVER from 00:1e:8c:6a:72:56 via 193.255.174.129: network 193.255.174.128
2010-05-19T00:05:58+03:00 fener dhcpcd: DHCPINFORM from 10.60.15.25 via 10.60.15.1
2010-05-19T00:05:58+03:00 fener dhcpcd: DHCPACK to 10.60.15.25 (00:0f:fe:e6:13:dc) via em0
2010-05-19T00:05:59+03:00 fener dhcpcd: DHCPREQUEST for 10.60.15.19 from 00:0f:fe:e6:65:55 (ekoPC_20-PC) via 10.60.15.1
2010-05-19T00:05:59+03:00 fener dhcpcd: DHCPACK on 10.60.15.19 to 00:0f:fe:e6:65:55 (ekoPC_20-PC) via 10.60.15.1
2010-05-19T00:06:01+03:00 fener dhcpcd: DHCPREQUEST for 10.60.15.25 from 00:0f:fe:e6:13:dc (ekoPC_12-PC) via 10.60.15.1
2010-05-19T00:06:01+03:00 fener dhcpcd: DHCPACK on 10.60.15.25 to 00:0f:fe:e6:13:dc (ekoPC_12-PC) via 10.60.15.1
2010-05-19T00:06:02+03:00 fener dhcpcd: DHCPREQUEST for 10.60.15.4 from 00:0f:fe:e6:13:00 (ekoPC_21-PC) via 10.60.15.1
2010-05-19T00:06:02+03:00 fener dhcpcd: DHCPACK on 10.60.15.4 to 00:0f:fe:e6:13:00 (ekoPC_21-PC) via 10.60.15.1
2010-05-19T00:06:03+03:00 fener dhcpcd: DHCPINFORM from 10.5.0.2 via 10.5.0.1
2010-05-19T00:06:03+03:00 fener dhcpcd: DHCPACK to 10.5.0.2 (00:00:00:00:00:00) via em0
2010-05-19T00:06:04+03:00 fener dhcpcd: DHCPINFORM from 10.35.0.159 via 10.35.0.1
2010-05-19T00:06:04+03:00 fener dhcpcd: DHCPACK to 10.35.0.159 (90:e6:ba:47:20:e3) via em0
```



Syslog'a Gönderilen FW Logları

- NAT logları
- URL Erişim Logları

```
File: messages.log      Line 277 Col 0      253269915 bytes
2010-05-19T00:07:08+03:00 193.140.143.1 %FWSM-5-304001: 10.70.0.48 Accessed URL 89.16.250.21:/resources/flavs/roulette.flv
2010-05-19T00:07:08+03:00 193.140.143.1 %FWSM-5-304001: 10.70.0.48 Accessed URL 208.64.178.130:/analiz.php3?kod=w&b=1&user=onlinefi&k=2&b
://www.google.com.tr/search?hl=tr&rlz=1W1GGLL_en&q=2012+filmini+izle&aq=0&aql=g10&aql=&sq=2012+&gs_rfai=&l=http://www.onlinefilmci.com/on
amet-Gunu-Macara-filmini-izle.html&w=1280&h=1024
2010-05-19T00:07:08+03:00 193.140.143.1 %FWSM-5-304001: 10.70.0.48 Accessed URL 75.126.182.188:/sa.js?_salogin=tptr&_sav=4.1
2010-05-19T00:07:08+03:00 193.140.143.1 %FWSM-6-305011: Built dynamic tcp translation from inside:10.70.0.48/64080 to outside:193.255.177
2010-05-19T00:07:08+03:00 193.140.143.1 %FWSM-6-305011: Built dynamic tcp translation from inside:10.70.0.48/64081 to outside:193.255.177
2010-05-19T00:07:08+03:00 193.140.143.1 %FWSM-5-304001: 160.75.181.206 Accessed URL 193.140.143.7:/duyuru/122/geleneksel-bahar-senligi--2
2010-05-19T00:07:08+03:00 193.140.143.1 %FWSM-6-305012: Teardown dynamic tcp translation from inside:10.60.6.123/49444 to outside:193.255
n 0:00:30
2010-05-19T00:07:08+03:00 193.140.143.1 %FWSM-5-304001: 160.75.181.206 Accessed URL 193.140.143.7:/css/screen.css
2010-05-19T00:07:08+03:00 193.140.143.1 %FWSM-5-304001: 160.75.181.206 Accessed URL 193.140.143.7:/js/jquery-1.3.2.min.js
2010-05-19T00:07:08+03:00 193.140.143.1 %FWSM-5-304001: 160.75.181.206 Accessed URL 193.140.143.7:/img/marmara_universitesi.gif
2010-05-19T00:07:08+03:00 193.140.143.1 %FWSM-5-304001: 160.75.181.206 Accessed URL 193.140.143.7:/img/marmara_logo.gif
2010-05-19T00:07:08+03:00 193.140.143.1 %FWSM-5-304001: 193.140.143.6 Accessed URL 74.125.87.101:/complete/search?hl=tr&client=hp&expIds=
46&q=ontol&cp=5
2010-05-19T00:07:08+03:00 193.140.143.1 %FWSM-5-304001: 160.75.181.206 Accessed URL 193.140.143.7:/img/sks.gif
2010-05-19T00:07:08+03:00 193.140.143.1 %FWSM-5-304001: 83.66.116.242 Accessed URL 193.140.143.15:/webmail/giris_12.gif
2010-05-19T00:07:08+03:00 193.140.143.1 %FWSM-6-305011: Built dynamic tcp translation from inside:10.70.0.48/64083 to outside:193.255.177
2010-05-19T00:07:08+03:00 193.140.143.1 %FWSM-5-304001: 83.66.116.242 Accessed URL 193.140.143.15:/webmail/giris_15.gif
2010-05-19T00:07:08+03:00 193.140.143.1 %FWSM-5-304001: 10.70.0.48 Accessed URL 84.22.127.26:/embed/pcrsc1bsybz5k/?/?width=470&height=306
2010-05-19T00:07:08+03:00 193.140.143.1 %FWSM-6-305012: Teardown dynamic udp translation from inside:10.100.0.166/62386 to outside:193.25
ion 0:00:30
```



Log'ların imzalanması

- » **Zaman Damgası**, belli bir verinin belirtilen bir tarihte var olduğunu kanıtlar.
- » 5070 sayılı elektronik imza kanunda belirtilen niteliklere sahip Zaman Damgası Sunucusu: <http://zd.kamusm.gov.tr>
- » C:\ZamaneConsole-1.1.7>java -jar ZamaneConsole-1.1.9.jar -z ornek.txt
<http://zd.kamusm.gov.tr> 80 username password

»veya

»OPENSSL TS

- » <http://www.openssl.org/source/openssl-0.9.8c.tar.gz>
- » http://www.opentsa.org/ts/ts-20060923-0_9_8c-patch.gz
- » Openssl 1.0.0 (ts'li sürüm) veya üstü



OpenSSL (>1.0.0)ile Zaman Damgası

```
#tar -xzvf openssl-1.0.0.tar.gz
#cd  openssl-1.0.0
#./config
#make install
#mkdir /ca
#chmod -R 0700 /ca
#cd /ca
#mkdir private
#mkdir newcerts
#echo '99999' > #serial
#touch index.txt
```



openssl.cnf

```
--- ./openssl-1.0.0/apps/openssl.cnf 2009-04-04 21:09:43.000000000 +0300
+++ ../ssl/openssl.cnf 2010-05-22 19:31:34.000000000 +0300
@@ -39,7 +39,7 @@
#####
[ CA_default ]

-dir      = ./demoCA      # Where everything is kept
+dir      = /ca           # Where everything is kept
certs     = $dir/certs    # Where the issued certs are kept
crl_dir   = $dir/crl      # Where the issued crl are kept
database  = $dir/index.txt # database index file.
@@ -187,6 +187,8 @@
# This is typical in keyUsage for a client certificate.
# keyUsage = nonRepudiation, digitalSignature, keyEncipherment

+keyUsage = nonRepudiation, digitalSignature
+
# This will be displayed in Netscape's comment listbox.
nsComment = "OpenSSL Generated Certificate"
```



openssl.cnf

```
@ @ -212,7 +214,7 @ @  
#nsSslServerName
```

```
# This is required for TSA certificates.  
-# extendedKeyUsage = critical,timeStamping  
+extendedKeyUsage = critical,timeStamping
```

```
[ v3_req ]
```

```
@ @ -327,7 +329,7 @ @  
[ tsa_config1 ]
```

```
# These are used by the TSA reply generation only.  
-dir      = ./demoCA      # TSA root directory  
+dir      = /ca           # TSA root directory  
serial    = $dir/tsaserial # The current serial number (mandatory)  
crypto_device = builtin   # OpenSSL engine to use for signing  
signer_cert = $dir/tsacert.pem # The TSA signing certificate
```



KÖK sertifikaların oluşturulması

Diğer sertifikaların oluşturulmasında kullanılacak ana sertifikanın oluşturulması

```
#openssl req -new -x509 -newkey \
rsa:2048 -days 3650 -out cacert.pem \
-keyout private/cakey.pem
```

Enter PEM pass phrase	: parola123
Country Name	: TR
State or Province Name	: Anadolu
Locality Name	: Istanbul
Organization Name	: Marmara Universitesi
Organizational Unit Name	: BIM
Common Name	: Sistem Sorulusu
Email Address	: sysadmin@marmara.edu.tr



TSA (Time Stamping Authority) Sertifikaları

TSA için gizli anahtarı oluşturulması

```
#openssl genrsa -aes256 -out tsakey.pem 2048
```

TSA için sertifika otoritesinden sertifika istemek için isteğin oluşturulması

```
# openssl req -new -key tsakey.pem -out tsareq.csr  
Enter pass phrase for tsakey.pem: parola123
```

TSA için CA dan sertifika isteme; daha önceden oluşturulmuş ana sertifika kullanılarak TSA'nın gizli anahtarına uygun sertifikanın üretilmesi

```
#openssl ca -days 3650 -in ca/tsareq.csr \  
-out ca/tsacert.pem  
#mv ca/tsakey.pem ca/private/
```



TSA ile Dosyanın İmzalanması

İmzalanacak dosya için isteğin (dosya) oluşturulması;

```
#/usr/local/bin/ssl/openssl ts -query -data dosya_adi \  
-no_nonce -out dosya_adi.tsq
```

Damga istek dosyasının okunabilir çıktısı

```
#/usr/local/ssl/bin/openssl ts -query -in dosya_adi.tsq -text
```

Response oluşturulması – imzalama:

```
#/usr/local/ssl/bin/openssl ts -reply -queryfile \  
dosya_adi.tsq -out dosya_adi.tsr -token_out -config \  
/usr/local/ssl/openssl.cnf -passin pass:parola123
```



Doğrulama

```
# /usr/local/ssl/bin/openssl ts -verify -data dosya_adi -in \  
dosya_adi.tsr -token_in -CAfile cacert.pem -untrusted tsacert.pem
```

"dosya_adi" dosyası, damgalanmış olan ve şu an damga ile uyumlu olup olmadığı kontrol edilen veri dosyası

"**dosya_adi.tsr**" dosyası, sunucudan gelen damga dosyası

"**cacert.pem**" dosyası, sunucu tarafından dağıtılan CA için public sertifika

"**tsacert.pem**" dosyası, sunucu tarafından dağıtılan TSA için public sertifika



Raporlama

```
#!/bin/sh
gun=`date -v -1d +%d`
ay=`date -v -1d +%m`
yil=`date -v -1d +%Y`
#
# fw logu dizinine git
#
cd /data/logs/syslog/$yil/$ay/$gun/193.140.143.1
#
# zaman sunucusundan zamanı guncelle
ntpdate 193.140.143.2 > ../sonuc
#
# logu imzala
/usr/local/ssl/bin/openssl ts -query -data messages.log -no_nonce -out messages.tsq
/usr/local/ssl/bin/openssl ts -reply -queryfile messages.tsq -out messages.tsr -token_out -
config /usr/local/ssl/openssl.cnf -passin pass:1q2w3e4r
#
# tarih dizinine, yani ana dizine sonuc dosyasına dosyaların durumunu yaz
#
pwd >> ../sonuc
ls -l >> ../sonuc
#
```



Raporlama

```
# dogrula ve sonucunu ayni dosyaya yaz
#
/usr/local/ssl/bin/openssl ts -verify -data messages.log -in messages.tsr -token_in -
CAfile /CA/cacert.pem -untrusted /CA/tsacert.pem >> ../sonuc
#
# ayni islemleri dhcp icin uygula
#
cd ../fener
/usr/local/ssl/bin/openssl ts -query -data messages.log -no_nonce -out messages.tsq
/usr/local/ssl/bin/openssl ts -reply -queryfile messages.tsq -out messages.tsr -token_out
-config /usr/local/ssl/openssl.cnf -passin pass:1q2w3e4r
pwd >> ../sonuc
ls -l >> ../sonuc
/usr/local/ssl/bin/openssl ts -verify -data messages.log -in messages.tsr -token_in -
CAfile /CA/cacert.pem -untrusted /CA/tsacert.pem >> ../sonuc
#
# sonucu ilgililere postala
#
ALICI="admin1@marmara.edu.tr admin2@marmara.edu.tr"
POSTAGONDER="/usr/bin/mail -s"
KONU="TS İmza"
$POSTAGONDER "$KONU" "$ALICI" < ../sonuc
```



Rapor Sonucu

30 Nov 01:30:05 ntpdate[82458]: step time server 193.140.143.? offset 3.993856 sec

/data/logs/syslog/2010/11/29/192.168.169.170

total 5084136

-rw-r--r-- 1 root wheel 2601767702 Nov 30 00:00 messages.log

-rw-r--r-- 1 root wheel 40 Nov 30 01:30 messages.tsq

-rw-r--r-- 1 root wheel 907 Nov 30 01:30 messages.tsr

Verification: OK

/data/logs/syslog/2010/11/29/fener

total 40616

-rw-r--r-- 1 root wheel 20764823 Nov 30 00:00 messages.log

-rw-r--r-- 1 root wheel 40 Nov 30 01:30 messages.tsq

-rw-r--r-- 1 root wheel 907 Nov 30 01:30 messages.tsr

Verification: OK



teşekkürler

huseyin @ marmara.edu.tr

