BGA
BİLGİ GÜVENLİĞİ AKADEMİSİ
www.bga.com.tr

Bilişim Sistemlerinde Adli Bilişim Analizi ve Bilgisayar Olayları İnceleme - 101

Huzeyfe ÖNAL

Bilgi Güvenliği AKADEMİSİ

Huzeyfe.onal@bga.com.tr

Açıklama

- Bu sunum Computer Forensic ile ilgili detaylara değinmemektedir. Computer forensic çok geniş bir alan olup her konuda uzman olmak (bilgi sahibi olmak değil)günümüz koşullarında çok talep edilen fakat pratik olarak pek de mümkün olmayan bir durumdur.
- Sunum genelinde daha az önem verilen “Network Forensics” ve “Olay İnceleme” konusuna ağırlık verilecektir.

Ajanda

- Genel Tanımlar
- Adli Bilişim ve Günümüzdeki Önemi
- T.C.K'daki Kanunlar ve Uygulama Alanları
- Adli Bilişim Çeşitleri
- Adli Bilişim Çalışmalarında Dikkat Edilesi Hususlar
- Ağ Sistemlerine Yönelik Adli bilişim Çalışmaları
- Örnek Olay İnceleme
  - Hacklendiğinizden nasıl haberiniz olur?
  - Hacklendiğinizden haberdar mısınız?

Bilişim Kavramı

- Bilişim nedir?
  - İnsanların; teknik, ekonomik ve toplumsal alanlardaki iletişimlerinde kullandıkları, bilimin dayanağı olan bilginin, özellikle elektronik makinalar aracılığıyla düzenli ve akılcı biçimde işlenmesi, *bilginin elektronik cihazlarda toplanması ve işlenmesi bilimi.*

Bilgisayar Kavramı

- Bilgisayar Nedir?
  - Çok sayıda aritmetiksel veya mantıksal işlemlerden oluşan *bir işi önceden verilmiş bir programa göre yapıp sonuçlandıran*, *bilgileri depolayan* elektronik araç, elektronik beyin

Bilişim Suçu Tanımı

- *Herkes tarafından kabul edilen net bir tanımı olmamakla birlikte* Avrupa Ekonomik Topluluğu Uzmanlar Komisyonu'nun Mayıs 1983 tarihinde Paris Toplantısı'nda aşağıdaki şekilde tanımlamıştır.
- *"Bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde gayri kanuni, gayri ahlaki veya yetki dışı gerçekleştirilen her türlü davranış"*

Bilişim Suçları

- Çoğu zaman birbiri yerine kullanılsa da aralarında farklılıklar bulunan çeşitli kavramlar:
  - A)Bilgisayar suçu,
  - B)Bilgisayarla ilgili suç,
  - C)Bilgisayar suçluluğu,
  - D)Elektronik suç,
  - E)Bilgisayar vasıtası ile işlenen suçlar,
  - F)Bilişim suçları ya da suçluluğu,
  - G)Bilişim ihlali,

Bilişim Suçları-II

- Avrupa Ekonomik Topluluğu bilişim suçlarını 5'e ayırmıştır.
  1. Bilgisayarda mevcut olan kaynağa veya herhangi bir değere gayri meşru şekilde ulaşarak transferini sağlamak için kasten bilgisayar verilerine girmek,bunları bozmak,silmek,yok etmek,
  2. Bir sahtekarlık yapmak için kasten bilgisayar verilerine veya programlarına girmek,bozmak,silmek,yok etmek,
  3. Bilgisayar sistemlerinin çalışmasını engellemek için kasten bilgisayar verilerine veya programlarına girmek,bozmak,silmek,yok etmek,
  4. Ticari manada yararlanmak amacı ile bir bilgisayar programının yasal sahibinin haklarını zarara uğratmak,
  5. Bilgisayar sistemi sorumlusunun izni olmaksızın,konulmuş olan emniyet tedbirlerini aşmak sureti ile sisteme kasten girerek müdahalede bulunmaktır.

Bilişim Suçu Örnekleri

LC WAİKİKİ'DEN İFTİRAYA İLANLI YANIT

Tema Mağazacılık, bünyesindeki LC Waikiki, markasını karalamaya yönelik yapıldığını açıkladığı elektronik posta bildirisinin izlerini silmek ve Türkiye Cumhuriyeti'nin değerlerine bağlılığını göstermek için bu kez gazetelere "Cumhuriyet Bayramı'nı kutlama" ilanı verdi.

GAZETECİ HAKAN ÇELİK'TEN NE İSTİYORLAR?

İnternette büyük oyun!

10.10.2008 00:00

Karakter boyutu : A A

Posta Gazetesi Ankara Temsilcisi Hakan Çelik, kendi adıyla internette dolaşan ve "Bir Türk olarak Kürtlere soruyorum" başlığını taşıyan yazının kesinlikle kendisine ait olmadığını açıkladı. Hakan Çelik, e- mail yoluyla yayılan

O Kaset Kanada'dan Yüklenmiş!

10.05.2010 16:20

Metacafe'ye yüklenen Baykal'ın görüntülerinin Kanada Toronto merkezli bir adrese sahip olduğu öne sürülüyor.

mehmetali06168@hotmail com error verdi.

30 Mart 2010, 12:43 Anadolu Haber

Geçtiğimiz haftalarda siyasetin merkezi Ankara`yı karıştıran `Bomba yüklü kamyon` ihbarını yapan `mehmet ali` rumuzlu kişi Cumhuriyet Başsavcılığı

Facebook, Türkiye`de suç aleti oldu

Facebook rüvası kabus oldu. Sitede kan davalısına

Teklan ile Siberalem Arasında dDOS Tartışması

Yazan: Metin Y?lmaz | 22 Ağustos 2007, Çarşamba | Sayfayı Yazdır | Tavsiye Et | Paylaş

EBI firması, kendisine dDOS saldırısı yapıldığı suçlamasıyla Teklan aleyhine beyoğlu Cumhuriyet Savcılığına şikayette bulundu. Şirketin itiraf.com, siberalem benzeri sitelerinin host edildiği firma olan Teklan'dan ayrılmak istemesi üzerine saldırıların başladığı iddiası, sektörü karıştırdı. Teklan konuyla ilgili bir açıklama yaparak, olayı yalanladı.

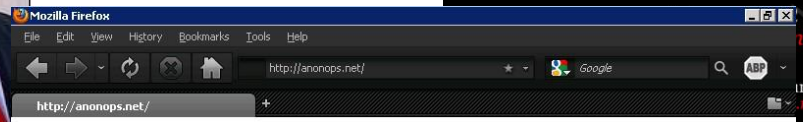
Anonymous TİB'e saldırdı!

**Dün akşam saatlerindeTürkiye'de bazı kamu kurumlarına siber sal
bulunan siber-aktivistler grubu Anonymous, ilk hedef olarak TİB'i s
Oluşum Meteorolojinin ve SGK'nın da sitelerini hedef aldı.**

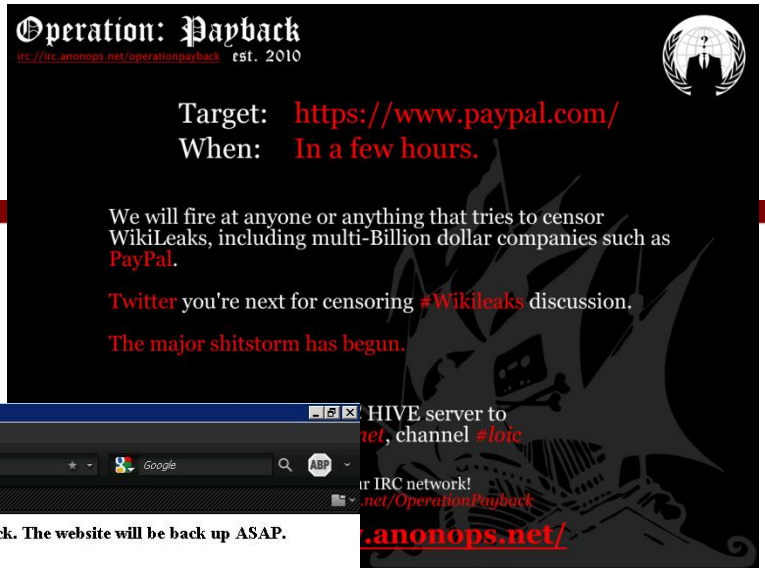
ntvmsnbc ve Ajanslar
Güncelleme: 20:22 TSİ 09 Haziran. 2011 Perşembe

İSTANBUL - Uluslararası siber-aktivistler grubu Anonymous'un Türkiye'de yürürlüğe girecek filtre uygulamasını protesto için yapacağını açıkladığı ilk siber saldırı, dün akşam saatlerinde gerçekleşti ve ilk olarak Telekomünikasyon ve İletişim Başkanlığı'nın sitesini hedef aldı.

Başkanlığın yedek sunucular da dahil 8 ayrı önlemine rağmen, siteye 18:00'den itibaren yaklaşık 20 dakika erişilemedi.



AnonOps is currently under heavy DDoS attack. The website will be back up ASAP.



DDoS Saldırı Örneği

Siberalem.com, itiraf.com ve ideefixe.com sitelerine ATAK YAPARAK çalışamaz hale getirdiği iddia edilen kişi yakalandı; TUTUKSUZ YARGILANACAK

İlişkili Başlıklar Tüm Başlıklar

- İnternet Bilgisayar Korsanlığı - Hackerlık (132 haber)
- İnternet Suçları (129 haber)
- İnternet (731 haber)

Bu Başlığı Takip Et | Haberi Sakla

Paylaş :

Bilgisayar Programcısı Batuhan Ç., "Benim bilgisayarımı kullanarak bu saldırıları yapmış olabilirler. Benim bunlarla bir alakam yok" dedi

Elektronik Bilgi İletişim şirketi yetkilileri, İstanbul Asayiş Şube Müdürlüğü'ne başvurarak, beş milyondan fazla üyesi bulunan kendilerine ait www.siberalem.com, www.itiraf.com ve www.ideefixe.com sitelerinin hacklenerek çalışmaz hale getirildiğir belirtip şikâyetçi oldular.

Bilişim Suçları Büro Amirliği ekipleri, "DDOS Attack" yöntemi kullanılarak kullanıcıların sisteme girmelerinin engellediğini tespit etti. Elektronik ortamda takibe alınan hackerın izini kısa sürede bulan dedektifler Batuhan Ç.'yi (26) önceki gün gözaltına aldı. Bilgisayar Programcısı Batuhan Ç., "Benim bilgisayarımı kullanarak bu saldırıları yapmış olabilirler. Benim bunlarla bir alakam yok" dedi. Poliste işlemleri tamamlandıktan sonra adliyeye çıkarılan Batuhan Ç. tutuksuz yargılanmak üzere serbest bırakıldı.

Hacklenen üç sitenin sahibi olan şirketin yetkilileri, 17 Temmuz 2007'de yaklaşık 22 aydır host hizmeti aldıkları şirketi pahalı olduğu için bırakacaklarını açıkladıklarını belirttiler. Şirket yetkilileri, bunun üzerine, host hizmeti aldıkları şirketin kendilerini, "Bizi bırakırsanız sizi batıracağız. Size karşı elektronik saldırılar düzenleyip sitelerinizi

Siber Dünyada Suç İşleme

- Çok kolay işlenir
- Birileri sizin adınıza sizin sistemlerinizden suç işleyebilir!
- Gerçek dünyaya oranla daha fazla iz bırakılır
- Gerçek dünyaya oranla izler daha kolay silinebilir
  - Her işlem mutlaka bir iz bırakır.
- Kendini gizleme şansı gerçek hayata oranla yüksektir
- Araç değil amaç önemlidir:
  - Bir ihbar mailiyle (Sms) tüm ülkeyi karıştırma
  - LCW hakkında yayılan mailler
    - Bilişim suçu bir amaç değil araç olarak kullanılmaktadır
    - Bakan akrabasının(!) ÖSYM başkanına gönderdiği e-posta

Adli Bilişim

- Adli bilişim, bilişim sistemleri üzerinden genellikle veri olarak elde edilen delillerin toplanması, saklanması, derlenmesi ve analizi konusunda ilke ve standartlar oluşturan multi disipliner yapıda yeni bir bilim dalıdır.
- Teknik ifadeyle:

Adli Bilişim; elektromanyetik-elektro optik ortam(lar)da muhafaza edilen ve/veya bu ortamlarca iletilen; ses, görüntü, veri/bilgi veya bunların birleşiminden oluşan her türlü bilişim nesnesinin, mahkemede sayısal (elektronik-dijital) delil niteliği taşıyacak şekilde: Tanımlanması, elde edilmesi, saklanması, incelenmesi ve mahkemeye sunulması çalışmaları bütünüdür.

http://www.hukukcu.com/bilimsel/kitaplar/bilisim_internet_suclari.htm

Adli Bilişim Analizi

- Bir konuda şeytanın aklına gelecek detayların bilinmesidir.
  - Suçlu psikolojisini tahmin etme ve tüm olasılıkları değerlendirme
- Çalışılan konu hakkında ne kadar detay bilgi varsa o kadar sağlıklı analiz raporu çıkarılabilir
  - Türkiye'den örnekler(Bilirkişi sorunları)
- Çeşitleri vardır.
  - Network forensics
  - Disk forensics
  - Mobile forensics
  - Memory forensics
  - ...

Adli Bilişim Analizi Neden Önemlidir?

- Artık her suçun mutlaka bilişim ayağı olmaktadır
- İnsanların basit sebeplerden dolayı suçlanması ya da basit bilgisizliklerden dolayı suçdan kaçmalarına sebep olabilir
- Sanal ortamlarda delil bırakma veya delilleri silme daha kolaydır.
- Sadece suç açısından değil bir ağ ortamında güvenlikle ilgili problemlerin çözümünde de yardımcı bir konudur.

Türkiye’de Adli Bilişim

- Türkiye’de Adli Bilişim denildiğinde akla gelen:

adım Selen. İzmir'de yaşıyorum. Adli tıp enstitüsünde yüksek lisans yapmaktayım.gelecekte bilgi teknolojileri bilişim suçları alanında bilirkişi olmak için kendimi eğitmek istiyorum.
Sizden, ya da beni yönlendireceğiniz kuruluştan öyle bir eğitim almak istiyorum ki,sonrasında mahkemeden bana sorulacak aşağıdaki sorulara yanıt verebileyim:
*bir bilgisar üzerinden kredi kartı online bankacılık dolandırıcılığı olmuştur.ve şüpheli web geçmişini temizlemiştir.gönderilen harddiske bakarak bu suçun bu bilgisayardan mı yapıldığını söyle.
*karı-koca bosanma davası.adam kadının facebook-hotmail-msn üzerinden baska erkeklerle gorustugunu soyluyor.ama kadın tum mesajlarını sılmıs.
msn konusma kaydını da hıc tutmamış.delil var mı?
*suca karısan bir IP tespit edilmiş.tam saati saniyesi internet sağlayıcıya bildirilmiş.internet sağlayıcı o saatte bu dınamık IP'nın xx e atandığını bıldırmıs.ancak kısı bunu ınkar ediyor.olası senaryolar?(wireless sifresi kırma,mac kodu ınternet saglayıcıda tutulur mu..vb gıbı sorular.)gercekten yaptıysa deliller?yapmadıysa delıller?
*çalınan bılgısayar,ethernet ya da wlan kartı MAC kodu bılınıyorsa bulunabılır mı?
*encase ile imaj alma.ve alınan bu ımajın analizi.
ve bunun gıbı aklınıza gelebılecek suç ile ilgili çeşitli sorular.

bu soruların hangilerinin cevabını kapsayan bir eğitimi bana verebilirsiniz?

Adli Bilişimcinin Temel Özellikleri

- Her konuda uzman olmamalı!
- Hukuki süreçler konusunda bilgili olmalı.
  - Hukuki yollardan elde edilmeyen deliller ne kadar önemli olsa da işe yaramayabilir.
- Günümüz sık kullanılan sistem, yazılım ve teknolojilerine hakim olmalı
  - Windows, facebook, msn, mail programları vs.

Adli Bilişim Çeşitleri

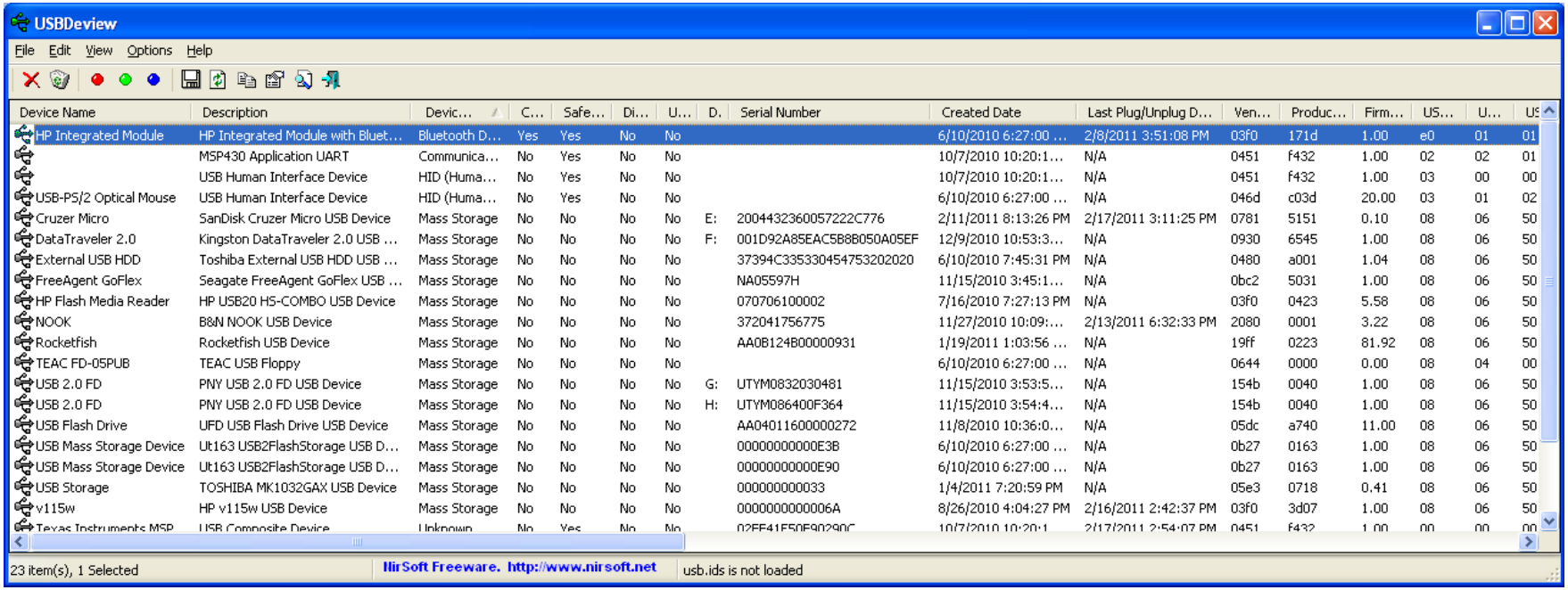
- Yeni bir alan olduğu için henüz sınırları belli, kabul edilmiş adli bilişim analiz çeşitleri yoktur
  - Geneline birden Computer forensics adı verilir
- Sektör tarafından bazı isimlendirmelerle çeşitler üretilmiştir
  - Disk forensics
  - Network forensics
  - Mobile forensics
  - Memory forensics
  - GSM forensics...

Disk Analizi

- Genellikle disk üzerinden silinmiş dosyaların geri getirilmesi veya gizlenmiş, bozulmuş önemli dosyaların kurtarılması amaçlı gerçekleştirilir.
  - Adli bilişim denildiğinde akla gelen ilk konudur.
- Disk çeşitleri ve yapısı iyi bilinmelidir
  - Pratik disk kullanımı: USB Bellekler
- İşletim sistemlerinin kullandığı dosya yapıları ve işleyişi iyi bilinmelidir.
- Disk silme işlemi
  - Geri getirilebilir mi?
  - Wipe
  - DoD standartları
  - US Department of Defense 5220.22-M

Örnek:Flash Bellek Analizi

- Takılan her USB cihaza ait detay bilgiler registry'de bir kayıt olarak tutulur.



Geri Getirilemez Silme İşlemi

- Geri getirilemez kavramı
  - Kime, neye göre geri getirilemez?

DoD standartları

- Linux shred komutu
  - 15/30 kere silme ve üzerine yazma
  - Komple diski silmek için
    - /dev/hda, /dev/sda parametre olarak verilmeli

```
root@bt:~# shred -n 15 ozel_dosya -v
shred: ozel_dosya: pass 1/15 (random)...
shred: ozel_dosya: pass 2/15 (924924)...
shred: ozel_dosya: pass 3/15 (b6db6d)...
shred: ozel_dosya: pass 4/15 (ffffff)...
shred: ozel_dosya: pass 5/15 (random)...
shred: ozel_dosya: pass 6/15 (000000)...
shred: ozel_dosya: pass 7/15 (249249)...
shred: ozel_dosya: pass 8/15 (random)...
shred: ozel_dosya: pass 9/15 (6db6db)...
shred: ozel_dosya: pass 10/15 (aaaaaa)...
shred: ozel_dosya: pass 11/15 (492492)...
shred: ozel_dosya: pass 12/15 (random)...
shred: ozel_dosya: pass 13/15 (db6db6)...
shred: ozel_dosya: pass 14/15 (555555)...
shred: ozel_dosya: pass 15/15 (random)...
root@bt:~#
```

Memory(Bellek) Analizi

- Son yıllarda ihtiyaç haline gelmiştir?
- Neden bellek analizi
  - Saldırgan logları silmiş olabilir
  - Disk üzerindeki dosyalar geri getirilmeyecek şekilde silinmiş olabilir.
  - Bellek başka bir proses dolduruncaya kadar eski proseslere ait bilgileri tutar
- Geçici veri depolama alanı olduğu için sistemin kapatılmaması gereklidir.
- Sadece Adli Bilişim değil saldırganlar için de önemli veri kaynağıdır.

Bellekten Neler Alınabilir?

```
Supported Plugin Commands:

        bioskbd         Reads the keyboard buffer from Real Mode memory
        connections     Print list of open connections [Windows XP Only]
        connscan2       Scan Physical memory for _TCPT_OBJECT objects (tcp connections)
        crashdump       Dumps the crashdump file to a raw file
        crashinfo       Dump crash-dump information
        dlldump         Dump DLLs from a process address space
        dlllist         Print list of loaded dlls for each process
        driverscan      Scan for driver objects _DRIVER_OBJECT
        files           Print list of open files for each process
        filescan        Scan Physical memory for _FILE_OBJECT pool allocations
        getsids         Print the SIDs owning each process
        hibdump         Dumps the hibernation file to a raw file
        hibinfo         Dump hibernation file information
        hivelist        Print list of registry hives.
        hivescan        Scan Physical memory for _CMHIVE objects (registry hives)
        imagecopy       Copies a physical address space out as a raw DD image
        imageinfo       Identify information for the image
        inspectcache    Inspect the contents of a cache
        kdbgscan        Search for and dump potential KDBG values
        kpcrscan        Search for and dump potential KPCR values
        linux_arp       print the ARP table
        linux_dmesg     gathers dmesg buffer
        linux_dump_map  gathers process maps
        linux_ifconfig  gathers active interfaces
        linux_list_open_files   lists open files
        linux_lsmod     gathers loaded kernel modules
        linux_mount     gathers mounted fs/devices
        linux_netstat   lists open files
        linux_proc_maps gathers process maps for linux
        linux_route     lists routing table
        linux_route_cache       lists routing table
        linux_task_list_ps      gathers active tasks by walking the task_struct->task list
        linux_task_list_psaux   gathers processes along with full command line and start time
        linux_tasklist_kmem_cache       gathers process through the kmem_cache
        memdump         Dump the addressable memory for a process
        memmap          Print the memory map
        moddump         Dump a kernel driver to an executable file sample
        modscan2        Scan Physical memory for _LDR_DATA_TABLE_ENTRY objects
        modules         Print list of loaded modules
        mutantscan      Scan for mutant objects _KMUTANT
        netscan         Scan a Vista, 2008 or Windows 7 image for connections and sockets
        patcher         Patches memory based on page scans
        printkey        Print a registry key, and its subkeys and values
        procexedump     Dump a process to an executable file sample
        procmemdump     Dump a process to an executable memory sample
        pslist          print all running processes by following the EPROCESS lists
        psscan          Scan Physical memory for _EPROCESS objects
        psscan2         Scan Physical memory for _EPROCESS objects
        pstree          Print process list as a tree
        regobjkeys      Print list of open regkeys for each process
        sockets         Print list of open sockets
        sockscan        Scan Physical memory for _ADDRESS_OBJECT objects (tcp sockets)
        ssdt            Display SSDT entries
        strings         Match physical offsets to virtual addresses (may take a while, VERY verbose)
        testsuite       Run unit test suit using the Cache
        thrdscan2       Scan physical memory for _ETHREAD objects
        vaddump         Dumps out the vad sections to a file
        vadinfo         Dump the VAD info
        vadtree         Walk the VAD tree and display in tree format
        vadwalk         Walk the VAD tree
        volshell        Shell in the memory image
```

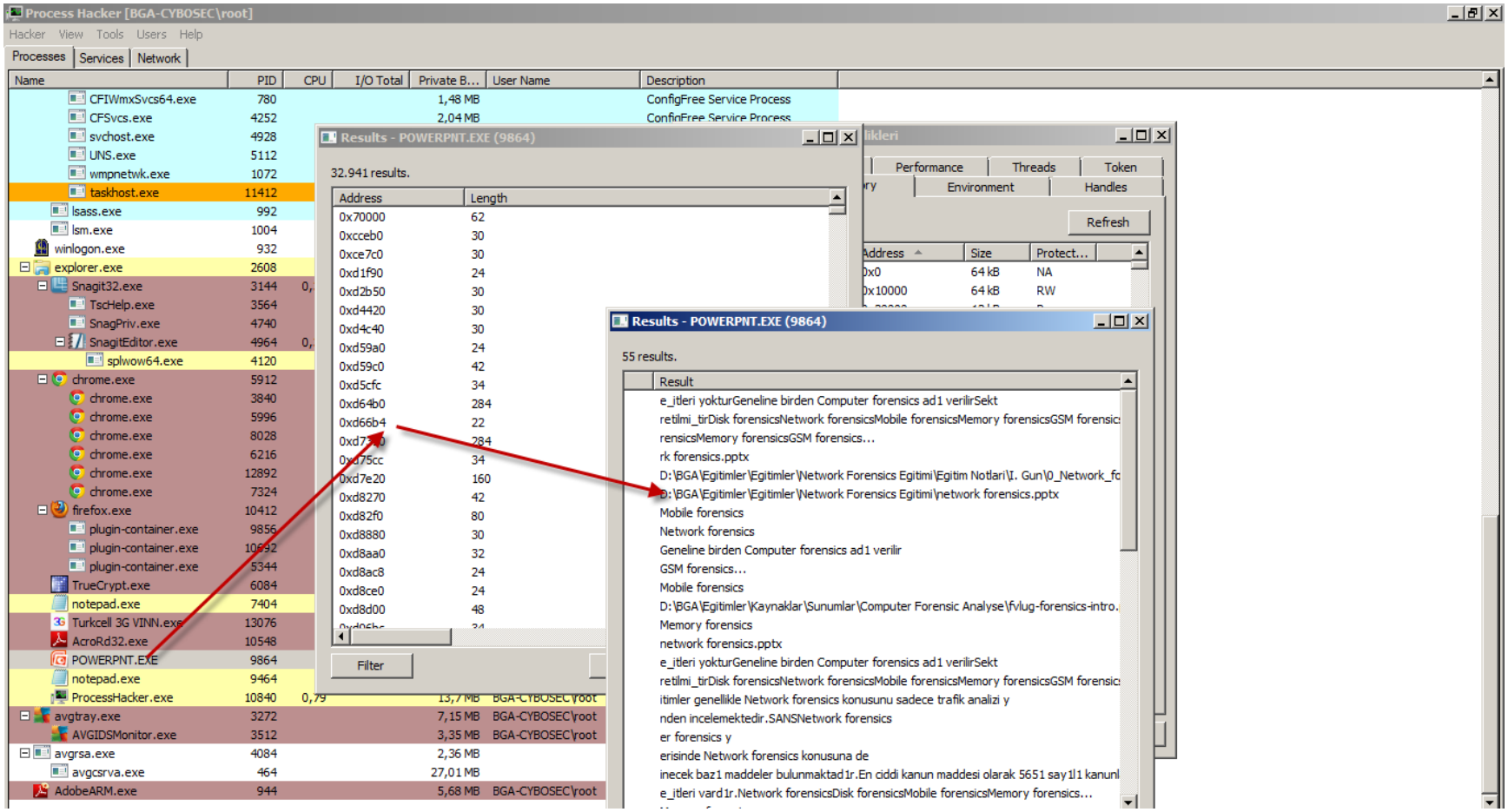
Linux Bellek Analizi

#memdump > FDUMP

- Alınan memory imajı düzensiz bir ikili dosyadır
  - İçerisinde tüm veriler ikili olarak tutulur
- Memdump ile dosyaya aktarılan hafıza bilgilerini string komutu ve grep komutunu kullanarak incelenebilir.

```
#strings FDUMP |grep netsec
netsec@192.168.1.107
netsec
sshd: netsec@pts/6
netsec
USER=netsec
MAIL=/var/mail/netsec
HOME=/home/netsec
LOGNAME=netsec
/var/mail/netsec
```

Windows Bellek Analizi



Profesyonel Analiz İçin

- Volatility

Basic Usage of Volatility 2.0

Volatility 2.0 has the ability to analyze W2K3 SP0/SP1/SP2, Vista SP0/SP1/SP2, W2K8 SP1/SP2 and Windows 7 SP0/SP1 images in addition to Windows XP SP2 and SP3. In order to analyze an image that is not Windows XP SP2, you should provide the correct profile when running Volatility commands. You can obtain the profile from Volatility by typing:

```
$ python vol.py --info
```

In addition to scanners, plugins and other items that Volatility "knows" about, you should see a section for profiles:

```
PROFILES
--------
VistaSP0x86  - A Profile for Windows Vista SP0 x86
VistaSP1x86  - A Profile for Windows Vista SP1 x86
VistaSP2x86  - A Profile for Windows Vista SP2 x86
Win2K3SP0x86 - A Profile for Windows 2003 SP0 x86
Win2K3SP1x86 - A Profile for Windows 2003 SP1 x86
Win2K3SP2x86 - A Profile for Windows 2003 SP2 x86
Win2K8SP1x86 - A Profile for Windows 2008 SP1 x86
Win2K8SP2x86 - A Profile for Windows 2008 SP2 x86
Win7SP0x86   - A Profile for Windows 7 SP0 x86
Win7SP1x86   - A Profile for Windows 7 SP1 x86
WinXPSP2x86  - A Profile for Windows XP SP2
WinXPSP3x86  - A Profile for windows XP SP3
```

Mobil Sistem Analizi

- Mobil sistemler hayatın her aşamasına girmiş durumda
  - Yakın gelecekte bilgisayarların yerini alması bekleniyor.
- Mobil sistemlere yönelik adli analiz çalışması neler içerir?
  - Cep telefonu, akıllı telefonların sistemleri, sim kart işlemleri
  - Sim kopyalama, akıllı telefon işletim sistemlerinin disk, memory analizi(iPhone iOS, Andreoid, Symbian)
- GSM ağı analizleri
  - Kim nereyi aradı, ne mesaj gönderdi, ne konuştu?
  - Dinleniyor muyum ☺

Mobil Sistem

- 3G ile birlikte mobil sistemler internetin ayrılmaz bir parçası haline gelmiştir.
- Artık her birey yürüyen bir “IP MAN”’e

Dönüşmüştür.

TCP/IP’deki problemler artık mobil sistemle

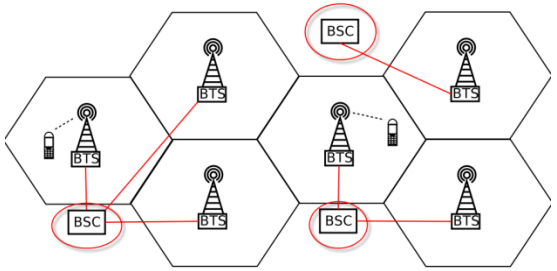
Kapsamaktadır.

GSM

- GSM (Global System for Mobile Communication
- 600 milyar dolarlık iş gücü
- 4.~ milyar kullanıcı
- %90 doyum oranına ulaşmış bir teknoloji

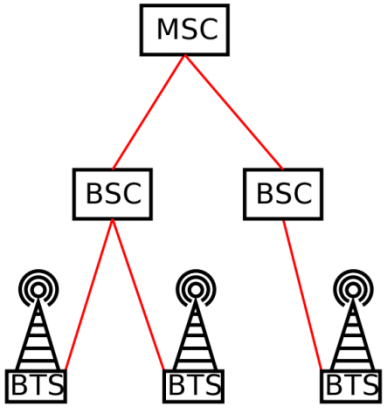
Temel GSM Bileşenleri

- MS
  - Mobile Station(Kullandığımız cep telefonları veya sim kart barındıran sistemler)
- BTS
  - Modulation/demodulation işlemlerini yapar
  - Layer 1 ve Rf Layer 2'nin bazı kısımlarını yönetir.
- BSC
  - Base Station Controller

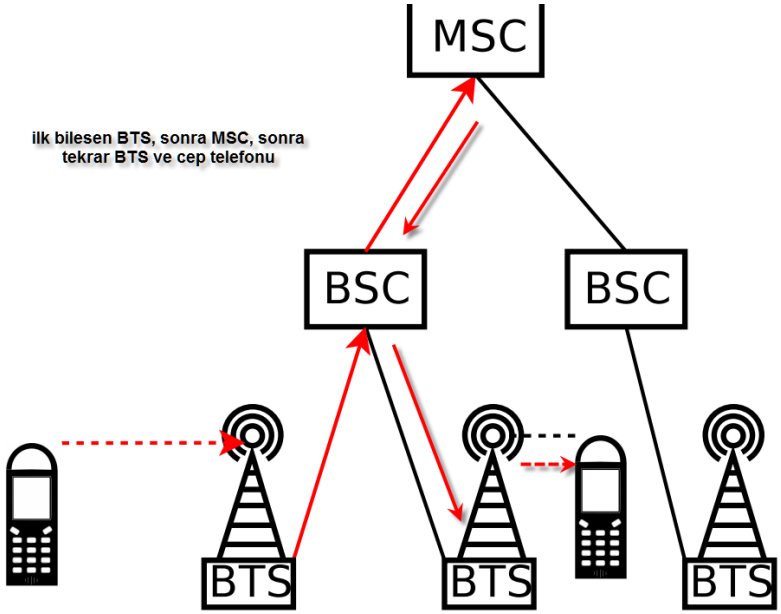


Temel GSM Bileşenleri-II

- MSC
  - Mobile Switching Center

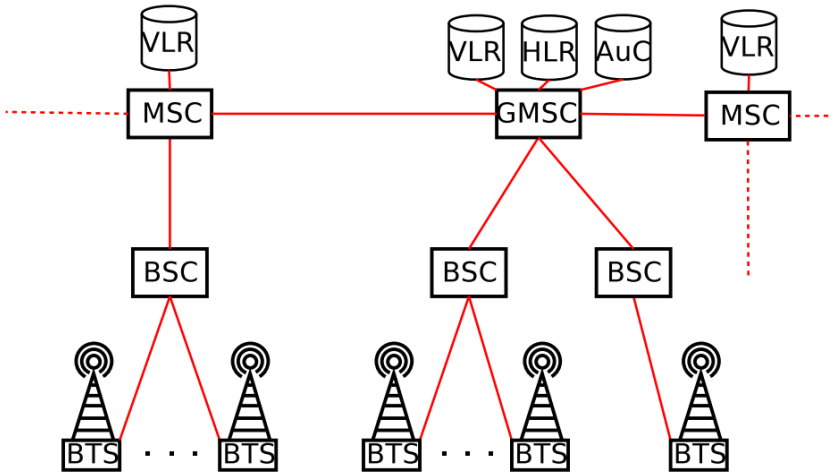


Telefon Arama İşlemi



Temel GSM Bileşenleri-III

- HLR ->Home Location Register
- VLR ->Visitor Locatin Register



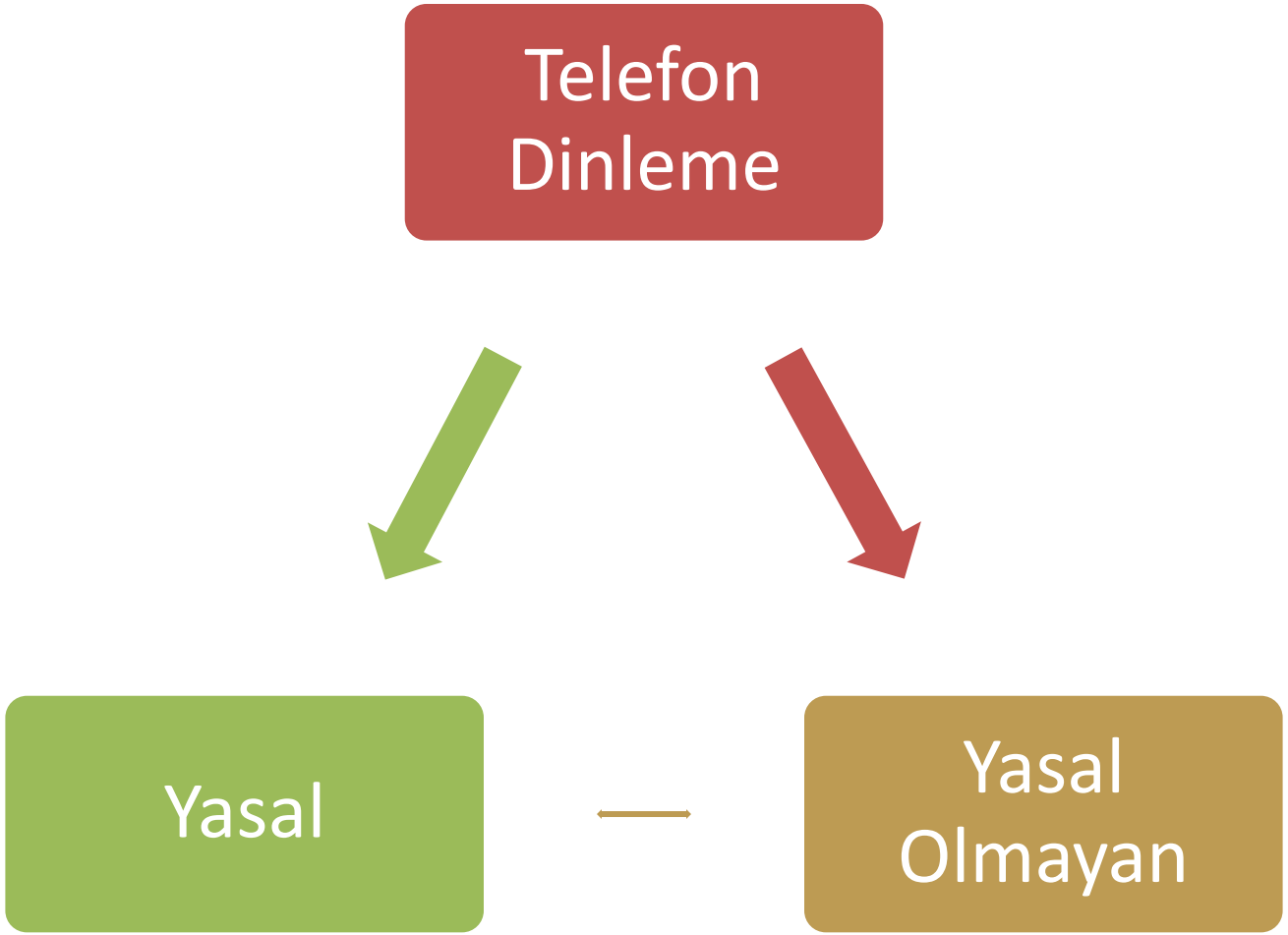
Mobil Sistemler Kullanılarak…

- Başkasının adına SMS gönderilebilir
- Başkasının telefon numarasından geliyormuş gibi çağrı bırakılabilir, arama yapılabilir
- Mobil telefonlara uzaktan yazılım yüklenebilir
- Mobil cihazlar uzaktan yönetilebilir, kamerası, mikrofonu açılabilir, disk üzerindeki tüm bilgiler edinilebilir

GSM Analizi İle Elde Edilebilecekler

- Kişinin güncel ve geçmişe yönelik lokasyon bilgileri
  - Her hafta sonu hangi eğlence mekanına gidiyor?
- Uyku saatleri, çalışma saatleri
- Arkadaşları, dostları ve vefasızları…

Telefon Dinleme



Yasal Telefon Dinleme

- Haberleşmenin Gizliliği Anayasa'nın 22. maddesi ile güvence altına alınmış olup, kişiler arasındaki haberleşmeye müdahale edilebilmesi ancak Anayasa'nın ilgili hükmü çerçevesinde, Kanun'la düzenlenen şartlarla ve yetkili mahkeme kararı ile mümkündür.

Yasal Telefon Dinleme-II

5397 sayılı yasa ve bu yasanın uygulama esaslarını düzenleyen Yönetmelik hükümleri gereği telekomünikasyon yoluyla yapılan iletişimin tespiti (arama, aranma, tarih, saat, yer bilgisi, vb.), dinlenmesi, sinyal bilgilerinin değerlendirilmesi ve kayda alınması işlemleri, 23.07.2006 tarihinden itibaren Bilgi Teknolojileri ve İletişim Kurumu(BTİK) bünyesinde faaliyete geçen Telekomünikasyon İletişim Başkanlığı (TİB) tarafından yürütülmektedir.

Konuya ilişkin GSM operatörlerinin bir sorumluluğu bulunmamakta olup TİB'e sadece teknik destek sağlanmaktadır.

Yasal Dinleme Nasıl Farkedilir?

- Yasal dinleme tamamen pasif bir dinleme yöntemi olduğu için dinlenen tarafların farketmesi pratik olarak mümkün değildir.

Telefon Görüşme Kayıtları(CDR)

- GSM operatörleri haberleşmenin gerçekleşmesi için gerekli altyapının kurulması, işletilmesi ve arızalarının giderilmesinden sorumludur.
- Dinleme ve kaydetme işlemi sadece yasal olarak tanımlanan süreçlerde ilgili devlet birimleri tarafından (TIB) gerçekleştirilir.
- Telefon Görüşme Kayıtları yasal olarak tutulmakta fakat telefon görüşme içerikleri tutulmamaktadır.
  - Call Details Record neler içerir?

CDR

- GSM operatörleri konuşmanın içeriği ile ilgili kayıt tutamazlar.
- Konuşma kayıtları terminolojisi GSM operatörlerinde hangi abonenin hangi numara ile kaç dakika ve saniye konuştuğunu gösteren kayıtlar için kullanılır.
- Bu bilgiler faturalama amacıyla ve ayrıntılı fatura iletiminde de kullanılır.

SMS Kayıtları

- Abone iletişim bilgileri GSM operatörleri tarafından izlenip kayıt altına alınamaz.
- Sadece kim, kime, ne zaman mesaj attı bilgisi kayıt ve faturalandırma amaçlı tutulmaktadır.

İllegal Telefon Dinleme

- Değişik yöntemleri vardır
- Genellikle pasif dinleme olarak gerçekleştirilir, farkedilmez
- Şifreleme algoritmalarının kullanımına göre değişebilir
- Authentication
  - A3
  - A8
- Şifreleme
  - A5/0
  - A5/1
  - A5/2
  - A5/3

Yazılım Aracılığıyla Telefon dinleme

- Günümüzdeki illegal dinlemelerin çoğu ortam dinlemesi ya da mobil sistemlere yüklenen casus yazılımlar aracılığıyla gerçekleştirilmektedir.

Network Forensics

- Ağ trafiği ve ağ sistemleri üzerinden delil toplama yöntemleri
- Yeni bir adli bilişim dalıdır
- Ağ bilgisi güçlü bir saldırgan için analizcileri şaşırtma, atlatma yöntemleri zor olmayacaktır
- Internet altyapısında kullanılan TCP/IP protokollerine bağımlı bir analiz biçimidir
  - Protokollerin eksiklikleri analiz aşamasında sağlıklı sonuçlar alınmasına engel olabilmektedir.

Network Forensics Farklılıkları

- Genelde diğer adli analiz yöntemlerine destek olma amacıyla kullanılır.
- Kayıtsız ve erişilebilir bir ortam olmadığı için saldırganın delilleri/kanıtları yok etme imkanı daha zordur
  - Tamamen pasif çalışan TAP sistemine erişim?
- Göreceli olarak daha fazla bilgi verir
- Henüz oturmuş, sınırları çizilmiş bir adli analiz biçimi değildir.

Neden Network Forensics?

- Günümüz kötücül yazılımları diske herhangi birşey yazmadan doğrudan bellekte çalışabiliyorlar.
  - Metasploit meterpreter
- Saldırgan işini bitirip çıktığında RAM ve ağ harici herhangi bir iz bırakmamış oluyor
- Saldırgan eriştiği sistemin loglarını silebilir
  - Bellekten bazı bilgilere erişim sağlanabilir
  - Saldırgan eriştiği sistemi tamamen silebilir
    - Bu durumda tek yol ağ/güvenlik kaynaklarından bilgi toplamak olacaktır.

Neden Network Forensics?-II

Open Source Hacking: Revealing Metasploit's Misdeeds

July 29, 2009
By Sean Michael Kerner
Submit Feedback »
More by Author »

One of the most devastating aspects of the open source metasploit vulnerability testing framework is meterpreter, which exploits a host machine in memory without leaving a trace. Meterpreter is supposed to be undetectable by IPS systems making it difficult if not impossible for someone to know what an attacker may have done to the victims' machine.

At the Black Hat security conference in Las Vegas, Mandiant security researchers Peter Silberman and Steve Davis are releasing a new forensic framework on Wednesday that will make it possible to detect whether or not a host was hit by Metapsloit's meterpreter. The new tool could change the game when it comes to Metasploit-based attacks that previously could not be identified on the target machine.

"Metasploit's meterpreter has been around since 2004 and it's a memory resident host exploitation module and because it's memory resident it breaks traditional disk forensics and the attacker leave no trace of the attack on the disk," Silberman said. "Our talk is how we can use memory forensics to reconstruct what an attacker has done with meterpreter to give analysts some idea of what has occurred."

In concert with the talk, the Mandiant researchers will release an open source tool called the Metasploit Forensic Framework. The goal of the tool is to make the undetectable, detectable. Metasploit itself is an open source vulnerability testing framework, but with meterpreter it has the stealth to evade most common security exploit detection mechanism.

```
{
system 'rm -rf /var/log/lastlog';
system "echo -e \"\\033[01;37m[*]/var/log/lastlog -erased Ok\"\n";
}
else
{
system "echo -e \"\\033[01;31m[*]/var/log/lastlog - No such file or directory\\033[01;37m\"\n";
}
if( -e "/var/log/wtmp" )
{
system 'rm -rf /var/log/wtmp';
system "echo -e \"\\033[01;37m[*]/var/log/wtmp -erased Ok\"\n";
}
else
{
system "echo -e \"\\033[01;31m[*]/var/log/wtmp - No such file or directory\\033[01;37m\"\n";
}
if( -e "/etc/wtmp" )
{
system 'rm -rf /etc/wtmp';
system "echo -e \"\\033[01;37m[*]/etc/wtmp -erased Ok\"\n";
}
else
{
system "echo -e \"\\033[01;31m[*]/etc/wtmp - No such file or directory\\033[01;37m\"\n";
}
if( -e "/var/run/utmp" )
{
system 'rm -rf /var/run/utmp';
system "echo -e \"\\033[01;37m[*]/var/run/utmp -erased Ok\"\n";
}
else
{
system "echo -e \"\\033[01;31m[*]/var/run/utmp - No such file or directory\\033[01;37m\"\n";
}
if( -e "/etc/utmp" )
{
system 'rm -rf /etc/utmp';
system "echo -e \"\\033[01;37m[*]/etc/utmp -erased Ok\"\n";
```

Network Forensics ve T.C Kanunları

- T.C.K'ları içerisinde Network forensics konusuna değinecek bazı maddeler bulunmaktadır.
- En ciddi kanun maddesi olarak 5651 sayılı kanunla birlikte gelen loglama maddeleridir
- Genellikle yanlış anlaşılır
- Network forensic kavramı paket/protokol demek olduğu için kimi yerlerde "özel hayatın gizliliği" ilkesiyle çakışır
  - Bu gibi durumlarda özel hayatın korunması ilkesi ağır basar.

5651 Sayılı Kanun

- 5651 sayılı “Internet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun” ve kanuna dayalı yürürlükteki yönetmelikler
- 2007 yılında tasarlandı
  - Aynı yıl içerisinde kanunun maddelerini daha anlaşılır hale getiren çeşitli yönetmelikler yayınlanarak yürürlüğe girdi
- Yerli “Big Brother” olarak algılandı
  - Teknik olarak yetersiz maddeler bulunmakta

5651 | Tanımlar

- **Erişim sağlayıcı:** İnternet toplu kullanım sağlayıcılarına ve abone olan kullanıcılarına internet ortamına erişim olanağı sağlayan işletmeciler ile gerçek veya tüzel kişileri.
  - *İnternet erişimi sağlayan ISP'ler, GPRS üzerinden internet erişim hizmeti veren GSM firmaları.*

Erişim Sağlayıcı Yükümlülükleri

- **Erişim sağlayıcı trafik bilgisi:** İnternet ortamına erişime ilişkin olarak abonenin adı, adı ve soyadı, adresi, telefon numarası, abone başlangıç tarihi, abone iptal tarihi, sisteme bağlantı tarih ve saat bilgisi, sistemden çıkış tarih ve saat bilgisi, ilgili bağlantı için verilen IP adresi ve bağlantı noktaları gibi bilgileri,

- a) Herhangi bir kullanıcısının yayınladığı hukuka aykırı içerikten, 5651 sayılı Kanun ve ilgili mevzuat hükümlerine göre Başkanlıkça haberdar edilmesi halinde ve teknik olarak engelleme imkânı bulunduğu ölçüde erişimi engellemekle,

Erişim sağlayıcı yükümlülükleri -II

- b) Sağladığı hizmetlere ilişkin olarak, Başkanlığın Kanunla verilen görevlerini yerine getirebilmesi için;

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

… ve ticari amaçla internet toplu kullanım sağlayıcılar için belirli bir IP bloğundan sabit IP adres planlaması yapmakla ve bu bloktan IP adresi vermekle,

Erişim sağlayıcı yükümlülükleri -III

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

- **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.

Erişim sağlayıcı yükümlülükleri -IV

- MSISDN-IP Logları:
  - MSISDN=Cep telefonu numarası
- Bu kanunda net yazılmamış fakat kanunun amacı göz önünde bulundurulduğunda olması gerekenlerden.
- Tanımı yapılan “**ERİŞİM SAĞLAYICI TRAFİK BİLGİSİ”** de abonenin telefon nosu ve adresi gibi bilgiler istenmekte.
- Bu bilginin verilebilmesi için MSISDN bilgisi tutulmalıdır.

5651|İçerik Sağlayıcı

- **İçerik sağlayıcı:** İnternet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişileri,
- Pratikte kimleri kapsar?
  - Site sahibi olup genele yayın yapan herkes.
  - E-posta listeleri, blogların sahibi de bu kapsama girmektedir.

İçerik Sağlayıcı Sorumlulukları

- İçerik sağlayıcı, internet ortamında kullanıma sunduğu her türlü içerikten sorumludur.
- İçerik sağlayıcı, bağlantı sağladığı başkasına ait içerikten sorumlu değildir. Ancak, sunuş biçiminden, bağlantı sağladığı içeriği benimsediği ve kullanıcının söz konusu içeriğe ulaşmasını amaçladığı açıkça belli ise, genel hükümlere göre sorumludur.

5651|Yer Sağlayıcı

- İnternet ortamında hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişileri,
- Hosting firmaları ya da benzeri işi yapan tüm firmalar

Yer Sağlayıcı Yükümlülükleri

- Yer sağlayıcı trafik bilgisini altı ay saklamakla, bu bilgilerin doğruluğunu, bütünlüğünü oluşan verilerin dosya bütünlük değerlerini (hash) zaman damgası ile birlikte saklamak ve gizliliğini temin etmekle, ...
- Yer sağlayıcı, yer sağladığı içeriği kontrol etmek veya hukuka aykırı bir faaliyetin söz konusu olup olmadığını araştırmakla yükümlü değildir.

Yer Sağlayıcı Yükümlülükleri-II

- **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,
- http, ftp ve smtp icin detay bilgi isteniyor.
  - Http ve ftp için url, Smtp için basit smtp başlık bilgileri.
- Log Türleri :

  HTTP log

  FTP log

  Mail log

Log Detayları

- İçerden dışarı yapılan bağlantılarda değil,
  - Özel hayatın gizliliğini ihlal ediyor
- Internete hizmet veren sistemlere gelen web, ftp ve mail paketleri için log isteniyor
- HTTP için
  - GET ve POST istek detayları
  - Web sunucu yazılımları POST detaylarını loglamaz
  - Ara sistemlere ihtiyaç vardır

5651|İnternet Toplu Kullanım Sağlayıcı

- Kişilere belli bir yerde ve belli bir süre internet ortamı kullanım olanağı sağlayan gerçek ve tüzel kişileri.
- Internet erişimi sağlayan her şirket bu kapsama giriyor. Halka açik kablosuz ağlar da bu kapsama girer.

İ.T.K Sağlayıcı Yükümlülükleri

- I.T.K=Internet Toplu Kullanım Sağlayıcı
- a) Konusu suç oluşturan içeriklere erişimi önleyici tedbirleri almak.
- b) İç IP Dağıtım Loglarını elektronik ortamda kendi sistemlerine kaydetmek.
  - DHCP logları
  - DHCP kullanılmıyorsa IP-MAC ikilileri

5651|Ticari Amaçlı 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 sağlayan gerçek ve tüzel kişileri,
- Internet kafeler

5651 Sayılı Kanun İncelemesi

- Kanunda temel olarak iki eksik nokta var:
  - Sayısal zaman damgasını kurumun kendisinin basıyor olması içeriğini istediği zaman değiştirip tekrar basabileceği anlamına gelir.
  - Genel olarak sistemlerin NAT yapısında çalıştığı düşünülürse suç işleyen bir şirket çalışanını bulmak neredeyse imkansızdır
- Neden?

Örnek Olay

- X şirketi çalışanı politik düşüncelerini ifade etmek için Y sitesine yorum yazıyor
- Y sitesindeki bu yorumu okuyan politikacının tepesi atıyor ve X şirketindeki bu şahsa dava açmak istiyor
  - Y sitesini barındıran firmadan loglar alınır
  - Yorumun yazıldığı saate bakılarak yorumun hangi ip adresinden geldiği belirlenir.
  - X firmasının IP adresi olduğu belirlenerek X firmasına gelinir
  - X firması güvenlik sistemlerinde NAT yapısı kullandığını belirterek istenen logları(DHCP, ip-mac) verir.
  - Analizi yapan mühendisin elinde yorumun yazıldığı saate dair NAT tablosu olmadığı için içerden kimin bu yorumu yazdığını bulamaz
  - Tüm bilgisayarların disk imajları alınarak merkeze götürülür…

Diğer TCK Maddeleri-I

Suçun Adı	Kanuni Dayanağı	Hapis Cezası Aralığı
Bilişim Sistemine Girme	TCK Md. 243	1 ila 2 Yıl arası hapis
Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme	TCK Md. 244	1 ila 6 yıl arası hapis
Banka ve Kredi Kartlarının Kötüye Kullanılması	TCK Md. 245	3 ila 8 yıl arası hapis
Ticari Sır, Bankacılık Sırrı veya Müşteri Sırrı Niteliğindeki Bilgi veya Belgelerin Açıklanması	TCK Md.239	1 ila 7 yıl arası hapis
Devletin Güvenliği veya İç veya Dış Siyasal Yararları Bakımından, Niteliği İtibarıyla, Gizli Kalması Gereken Bilgiler	TCK Md. 327, Md. 328, Md. 329	3 ila 20 yıl arası hapis(Savaş durumunda müebbet hapis)
Verilerin Kaydedilmesi	TCK Md. 135	6 ay ila 3 yıl arası hapis
Verilerin yok edilmesi	TCK Md. 138	6 ay ila 1 yıl arası hapis
Haberleşmenin gizliliğini ihlal	TCK Md. 132	6 ay ila 3 yıl arası hapis
Haberleşmenin engellenmesi	TCK Md. 124	6 ay ila 5 yıl arası hapis
Dolandırıcılık	TCK Md.158	3 yıl ila 7 yıl arası hapis

Diğer TCK Maddeleri-II

Bilişim Sistemleri Aracı Kılınarak İşlenen Suçlar

Suçun adı	Kanuni dayanağı	Hapis Cezası Aralığı
İntihara Yönlendirme	TCK Md. 84	2 ila 10 yıl arası hapis
Hakaret	TCK Md. 125	3 ay ila 2 yıl arası hapis
Hırsızlık	TCK Md. 142	3 ila 7 yıl arası hapis
Müstehcenlik	TCK Md. 226	3 ila 7 yıl arası hapis
Kumar Oynanması İçin Yer ve İmkân Sağlama	TCK Md. 228	1 yıla kadar hapis
Şantaj	TCK Md. 107	1 ila 3 yıl arası hapis
Tehdit	TCK Md. 106	6 ay ila 5 yıl arası hapis
Çocukların Cinsel İstismarı	TCK Md. 103	3 ila 8 yıl arası hapis
Uyuşturucu veya Uyarıcı Madde Kullanılmasını Kolaylaştırma	TCK Md. 190, 191	2 ila 5 yıl arası hapis
Sağlık İçin Tehlikeli Madde Temini	TCK Md. 194	6 ay ila 1 yıl arası hapis
Fuhuş	TCK Md. 227	4 ila 10 yıl arası hapis
Atatürk Aleyhine İşlenen Suçlar	5816 sayılı Kanun	1 ila 3 yıl arası hapis

Category:

Analiz Çalışmalarında Zaman Kavramı

- Adli bilişim analizi çalışmalarında en önemli bileşenlerden birisi zaman kavramıdır.
- Birden fazla ortamdan log/delil toplanacak bir yapıda en önemli unsur tüm sistemlerin zaman uyumudur.
  - Firewall, VPN sunucudan iki saat geri ise?

Zaman Kavramının Önemi

- BBP Genel başkanı kazası ve NTV örneği!
- Yanlış bilgilendirme ve ortalığın karışması!

Ölüm helikopterinde 139 defa arandı - Taraf/MEHMET

BARANSU - *Istanbul* - 22.10.2009

Cesedine dört günde ulaşılabilen BBP lideri Yazıcıoğlu'nun, helikopteri havalanır havalanmaz NTV santralinden 139 kez arandığı ortaya çıktı. Muhsin Yazıcıoğlu'nun Kahramanmaraş'ta öldüğü olayın kaza mı yoksa suikast mı olduğu günlerce tartışıldı. Taraf çok önemli yeni bilgilere ulaştı. Pilot ile İHA muhabirinin NTV santralinden toplam 150 kez arandığı biliniyordu. Aynı santralden Yazıcıoğlu, helikopterin havalanmasından kazaya kadar geçen sürede tam 139 kez, yanında bulunan BBP Sivas İl Başkanı ile yardımcısı da defalarca aranmış. Yazıcıoğlu'ndaki çağrıların hepsinin süresi sıfır saniye olarak gözüküyor. Helikopter düştükten sonra ise aramalar kesiliyor. Taraf'ın bilgisine başvurduğu telekomünikasyon sektöründe görevli iki mühendis, manyetik alan yaratılıp helikopterin düşürülmüş olabileceğini söyledi

GMT 0 Tarihi	TÜRKİYE SAATİ GMT +2	Arayan No	Aranan No	Süre
25.03.2009 14:34:36	25.03.2009 16:34:36	02123354161	905068543500	0
25.03.2009 14:41:02	25.03.2009 16:41:02	02123354161	905068543500	0
25.03.2009 14:47:16	25.03.2009 16:47:16	02123354163	905068543500	0
25.03.2009 14:47:27	25.03.2009 16:47:27	02123354163	905068543500	0
25.03.2009 14:48:17	25.03.2009 16:48:17	02123354163	905068543500	2
25.03.2009 14:48:34	25.03.2009 16:48:34	02123354163	905068543500	0
25.03.2009 14:48:48	25.03.2009 16:48:48	02123354163	905068543500	0
25.03.2009 14:49:21	25.03.2009 16:49:21	02123354163	905068543500	0
25.03.2009 14:49:52	25.03.2009 16:49:52	02123354163	905068543500	0
25.03.2009 14:50:01	25.03.2009 16:50:01	02123354163	905068543500	0
25.03.2009 14:50:28	25.03.2009 16:50:28	02123354163	905068543500	0
25.03.2009 14:50:31	25.03.2009 16:50:31	02123354163	905068543500	0
25.03.2009 14:50:35	25.03.2009 16:50:35	02123354163	905068543500	0
25.03.2009 14:50:57	25.03.2009 16:50:57	02123354163	905068543500	0
25.03.2009 14:52:02	25.03.2009 16:52:02	02123354163	905068543500	0
25.03.2009 14:52:09	25.03.2009 16:52:09	02123354163	905068543500	0
25.03.2009 14:52:43	25.03.2009 16:52:43	02123354163	905068543500	0
25.03.2009 14:53:20	25.03.2009 16:53:20	02123354163	905068543500	0
25.03.2009 14:54:01	25.03.2009 16:54:01	02123354163	905068543500	0

Anti Forensics

- Adli Bilişim Analizi çalışmalarını sekteye uğratma amaçlı kullanılan yöntemler bütünü.
- Bazı AF teknikleri farkedilebilir

Anti Forensics Teknikleri

- Bazı AF teknikleri:
- Disk için
  - Disk şifreleme yazılımlarının kullanımı
  - Disk üzerindeki dosyaların zaman ayarlarıyla oynama
  - Geri getirilemez disk/veri silme işlemleri
- Network forensic için:
  - Tünelleme
  - Encoding
  - Şifreleme - Gmail
  - Proxy kullanımı
  - IP spoofing
  - Güvenlik sistemlerini kandırma
  - Tuzak sistemler kullanma
  - Anonimleştirici ağlardan saldırı gerçekleştirme

Yararlanılan Kaynaklar

- Bu sunumdaki bazı tanımlar aşağıdaki web adreslerinde faydalanılarak hazırlanmıştır.

http://www.ahi-gurler-taygun.av.tr/?adli-bilisim-nedir-av.-m.gokhan-ahi,52

http://www.hukukcu.com/bilimsel/kitaplar/bilisim_internet_suclari.htm

Teşekkürler...