Sistem Güvenliği ve Port Reporter

MUSTAFA SERHAT DÜNDAR, <SERHAT AT SERHATDUNDAR DOT COM>,
21/06/2009

Port Reporter ; Windows Server 2003, Windows XP ve Windows 2000 çalışan bilgisayarlarda bir hizmet olarak çalışır. Araç TCP ve UDP bağlantı noktası etkinliğini günlüğe kaydeder.

- Aşağıdaki bilgileri loglayabilir :
- Kullanılan bağlantı noktaları
- Bağlantı noktalarını kullanan işlemler
- İşlemin bir hizmet olup olmadığı
- İşlemin yüklediği modüller
- İşlemi çalıştıran kullanıcı hesapları

Windows 2000 tabanlı bilgisayarlarda, hizmet, kullanılan bağlantı noktalarını ve ne zaman kullanıldıklarını günlüğe kaydeder.

Port Reporter aracı tarafından günlüğe kaydedilen bilgileri kullanarak bağlantı noktası kullanımını izleyebilir ve belirli sorunları giderebilirsiniz. Port Reporter aracı tarafından günlüğe kaydedilen bilgiler güvenlik açısından da yararlı olabilir. Bilgisayarımızın güvenliğini manual olarak incelemek için, yasal olarak şikayette bulunmak istediğimizde somut delil olarak log dosyalarını kullanabiliriz.

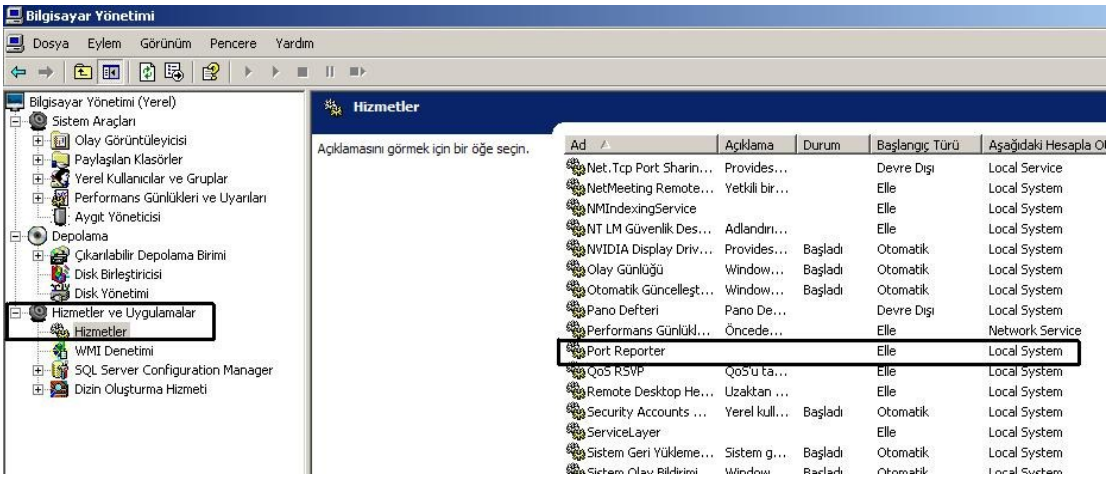
1) KURULUM

Port Reporter'i download etmek için "Referanslar" kısmındaki ilk bağlantıya tıklayabilirsiniz.

Port Reporter yazılımını install ettiğinizde C:\Program Files\PortReporter dizini altında PortReporter.exe dosyasını bulabilirsiniz.

Hizmeti başlatmak için Başlat\Çalıştır\services.msc yazıp Hizmetler penceresine ulaşın.

Hizmeti başlatmak için, hizmet adını tıklatın ve soldaki Başlat düğmesini tıklatın. Tamam'ı tıklatın.



Hizmetin başlangıç türünü "Otomatik" olarak seçiniz.

2) GÜVENLİK

Port Reporter Local System hesabını ile çalıştığı için, Port Reporter'ın yüklü olduğu klasörün güvenlik ayarlarını da yapmalıyız.

Port Reporter'ı yalnızca dosya sistemi NTFS olan bir bölüme yükleyin. FAT dosya sistemine Microsoft artık destek sağlamamaktadır.

C:\Program Files\PortReporter klasörüne sağ tıklayıp Özellikler'i seçin.

Güvenlik sekmesinden yetkilerin sadece SYSTEM ve ADMINISTRATOR'a ait olduğundan emin olun.

3) ÇALIŞMA AYARLARI

Başlat/Çalıştır penceresinde "services.msc" yazınız. Açılan hizmet penceresinde Port Reporter'i bulup çift tıklayın ve Hizmet Seçeneklerine ulaşın.

Başlangıç Parametreleri kısmına :

-ld ‘c:\loglar' yazıp onaylayınız. Artık loglarınız C:\WINDOWS\system32\Logfiles\PortReporter klasörü altında değil c:\loglar altında saklanacak.

-ls 10000 komutu ile log dosyalarının her birinin boyutunu belirlemiş olursunuz. 10bin KB. uygun bir değer.

4) Logging Özellikleri

Port Reporter hizmeti aşağıdaki durumlarda günlük dosyaları oluşturur:

- Port Reporter hizmeti her başladığında.
- Her gün gece yarısında.
- Günlük dosyasının boyutu 5 MB'ye veya başlangıç parametresinde belirttiğiniz özel boyuta ulaştığında.

Port Reporter hizmeti başladığında aşağıdaki günlük dosyaları oluşturulur:

- PR-INITIAL-*.log
- PR-PORTS-*.log
- PR-PIDS-*.log

Günlük dosyası adlarında dosyanın oluşturulduğu tarih ve saat (24 saat biçiminde) kullanılır. Tarih ve saat damgasının biçimi yıl-ay-gün-saat-dakika-saniye şeklindedir. Örneğin, aşağıdaki üç dosya 24 Ocak 2004 saat 8:49:30'da oluşturulmuştur:

- PR-INITIAL-04-01-24-8-49-30.log
- PR-PORTS-04-01-24-8-49-30.log
- PR-PIDS-04-01-24-8-49-30.log

5) PR-INITIAL günlük dosyası

PR-INITIAL günlük dosyası, Port Reporter hizmetinin, hizmet başlatıldığında bilgisayarda çalışan bağlantı noktaları, işlemler ve modüller hakkında topladığı bilgileri içerir. Her işlem için altında çalıştığı kullanıcı bağlamı da günlüğe kaydedilir. Aşağıda, Port Reporter hizmeti Windows XP tabanlı bir bilgisayarda başladığında oluşturulan örnek bir PR-INITIAL günlük dosyası bulunmaktadır:

Port Reporter Version 1.01 Log File
Service initialization log
System Date: Thu Jun 11 11:54:40 2009
Local computer name:
CLBR-E1614F7672 **// Bilgisayarınızın Kullanıcı İsmi**
Operating System: Windows XP **// İşletim Sisteminiz**
TCP/UDP Port to Process Mappings at service start-up
75 mappings found **// 75 Adet Bağlantı Yapılmış**
// Bazı bağlantıları editledim. Örnek olması açısında bir kısmını bıraktım.

PID:Process	Port	Local IP	State	Remote IP:Port
0:System Idle	TCP 3616	192.168.2.2	TIME WAIT	207.46.16.243:80

4:System TCP 445 0.0.0.0 LISTENING 0.0.0.0
400:alg.exe TCP 1025 127.0.0.1 LISTENING 0.0.0.0
804:ekrn.exe TCP 3618 192.168.2.2 ESTABLISHED 209.85.129.101:80
860:jqs.exe TCP 5152 127.0.0.1 CLOSE WAIT 127.0.0.1:3520
888:IBSocks.exe TCP 1034 192.168.2.2 ESTABLISHED *5.214.147.83:9001
988:ibhttp.exe TCP 8080 127.0.0.1 LISTENING 0.0.0.0
1500:lsass.exe UDP 500 0.0.0.0 *:*
2024:svchost.exe UDP 1900 192.168.2.2 *:*
2664:msnmsgr.exe TCP 2948 127.0.0.1 ESTABLISHED 127.0.0.1:30606
3424:firefox.exe TCP 3518 127.0.0.1 ESTABLISHED 127.0.0.1:3519
==========
==========
Process ID: 0 (System Idle)
System Idle Process **// Bağlantı Kurulmuş Portlar**
PID Port Local IP State Remote IP:Port
0 TCP 3603 127.0.0.1 TIME WAIT 127.0.0.1:30606
0 TCP 3615 127.0.0.1 TIME WAIT 127.0.0.1:30606
0 TCP 30606 127.0.0.1 TIME WAIT 127.0.0.1:3557
0 TCP 30606 127.0.0.1 TIME WAIT 127.0.0.1:3559
0 TCP 30606 127.0.0.1 TIME WAIT 127.0.0.1:3605
0 TCP 30606 127.0.0.1 TIME WAIT 127.0.0.1:3606
0 TCP 30606 127.0.0.1 TIME WAIT 127.0.0.1:3619
0 TCP 3592 192.168.2.2 TIME WAIT 63.88.212.184:80
0 TCP 3594 192.168.2.2 TIME WAIT 63.88.212.184:80
0 TCP 3604 192.168.2.2 TIME WAIT 207.46.16.243:80
0 TCP 3616 192.168.2.2 TIME WAIT 207.46.16.243:80
Port Statistics // Port İstatistikleri
TCP mappings: 11
UDP mappings: 0
TCP ports in a TIME WAIT state: 11 = 100.00%
Could not access module information for this process
==========
Loaded modules: **// Csrss.exe'ye ait çalıştırdığım .dll dosyaları**
(C:\WINDOWS\system32\csrss.exe (0x4A680000) dosyasına ait dll dosyaları)
C:\WINDOWS\system32\ntdll.dll (0x7C8F0000)
C:\WINDOWS\system32\CSRSRV.dll (0x75B20000)
C:\WINDOWS\system32\basesrv.dll (0x75B30000)
C:\WINDOWS\system32\winsrv.dll (0x75B40000)
C:\WINDOWS\system32\GDI32.dll (0x77F10000)
C:\WINDOWS\system32\KERNEL32.dll (0x7C800000)
C:\WINDOWS\system32\USER32.dll (0x7E360000)
C:\WINDOWS\system32\sxs.dll (0x75E70000)
C:\WINDOWS\system32\ADVAPI32.dll (0x77DC0000)
C:\WINDOWS\system32\RPCRT4.dll (0x77E70000)
C:\WINDOWS\system32\Secur32.dll (0x77FE0000)
C:\WINDOWS\system32\Apphelp.dll (0x77B30000)
C:\WINDOWS\system32\VERSION.dll (0x77BF0000)
==========
Process ID: 1488 (services.exe) **(Services.exe'nin kullandığı .dll dosyaları)**
User context: NT AUTHORITY\SYSTEM
Loaded modules:
C:\WINDOWS\system32\services.exe (0x01000000)
C:\WINDOWS\system32\ntdll.dll (0x7C8F0000)
C:\WINDOWS\system32\kernel32.dll (0x7C800000)
C:\WINDOWS\system32\msvcrt.dll (0x77C00000)
C:\WINDOWS\system32\ADVAPI32.dll (0x77DC0000)
C:\WINDOWS\system32\RPCRT4.dll (0x77E70000)
C:\WINDOWS\system32\Secur32.dll (0x77FE0000)
C:\WINDOWS\system32\USER32.dll (0x7E360000)

C:\WINDOWS\system32\GDI32.dll (0x77F10000)
C:\WINDOWS\system32\USERENV.dll (0x769B0000)
C:\WINDOWS\system32\SCESRV.dll (0x77B60000)
C:\WINDOWS\system32\AUTHZ.dll (0x776B0000)
C:\WINDOWS\system32\umpnpmgr.dll (0x7DB90000)
C:\WINDOWS\system32\WINSTA.dll (0x76340000)
C:\WINDOWS\system32\NETAPI32.dll (0x6FF90000)
C:\WINDOWS\system32\NCObjAPI.DLL (0x5FCC0000)
C:\WINDOWS\system32\MSVCP60.dll (0x76060000)
C:\WINDOWS\system32\ShimEng.dll (0x5D0A0000)
C:\WINDOWS\AppPatch\AcGenral.DLL (0x5A780000)
C:\WINDOWS\system32\WINMM.dll (0x76B30000)
C:\WINDOWS\system32\ole32.dll (0x774D0000)
C:\WINDOWS\system32\OLEAUT32.dll (0x77110000)
C:\WINDOWS\system32\MSACM32.dll (0x77BD0000)
C:\WINDOWS\system32\VERSION.dll (0x77BF0000)
C:\WINDOWS\system32\SHELL32.dll (0x7C9B0000)
C:\WINDOWS\system32\SHLWAPI.dll (0x77F60000)
C:\WINDOWS\system32\UxTheme.dll (0x5B2A0000)
C:\WINDOWS\system32\IMM32.DLL (0x76370000)
c:\progra~1\agnitum\outpos~1\wl_hook.dll (0x10000000)
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03\comctl32.dll (0x773C0000)
C:\WINDOWS\system32\comctl32.dll (0x5D5E0000)
C:\WINDOWS\system32\Apphelp.dll (0x77B30000)
C:\WINDOWS\system32\eventlog.dll (0x772F0000)
C:\WINDOWS\system32\WS2_32.dll (0x71AA0000)
C:\WINDOWS\system32\WS2HELP.dll (0x71A90000)
C:\WINDOWS\system32\PSAPI.DLL (0x76BE0000)
C:\WINDOWS\system32\wtsapi32.dll (0x76F40000)
==========
Process ID: 1920 (svchost.exe) **// Bilgisayarınızın Çalıştırdığı Servislerin Detaylı dökümü**
User context: NT AUTHORITY\SYSTEM
Service Name: AudioSrv
Display Name: Windows Ses
Service Type: shares a process with other services
Service Name: BITS
Display Name: Arka Plan Akıllı Aktarım Hizmeti
Service Type: shares a process with other services
Service Name: Browser
Display Name: Bilgisayar Tarayıcısı
Service Type: shares a process with other services
Service Name: CryptSvc
Display Name: Şifreleme Hizmetleri
Service Type: shares a process with other services
Service Name: Dhcp
Display Name: DHCP İstemcisi
Service Type: shares a process with other services
Service Name: dmserver
Display Name: Mantıksal Disk Yöneticisi
Service Type: shares a process with other services
Service Name: ERSvc
Display Name: Hata Bildirim Hizmeti
Service Type: shares a process with other services
Service Name: EventSystem
Display Name: COM+ Olay Sistemi
Service Type: shares a process with other services
Service Name: FastUserSwitchingCompatibility
Display Name: Hızlı Kullanıcı Değiştirme Uyumluluğu

Service Type: shares a process with other services
Service Name: helpsvc
Display Name: Yardım ve Destek
Service Type: shares a process with other services
Service Name: lanmanserver
Display Name: Sunucu
Service Type: shares a process with other services
Service Name: lanmanworkstation
Display Name: İş İstasyonu
Service Type: shares a process with other services
Service Name: Netman
Display Name: Ağ Bağlantıları
Service Name: Nla
Display Name: Ağ Konumu Tanıma (NLA)
Service Type: shares a process with other services
Service Name: RasMan
Display Name: Uzaktan Erişim Bağlantı Yöneticisi
Service Type: shares a process with other services
Service Name: Schedule
Display Name: Görev Zamanlayıcı
Service Type: shares a process with other services
Service Name: seclogon
Display Name: İkincil Oturum
Service Name: SENS
Display Name: Sistem Olay Bildirimi
Service Type: shares a process with other services
Service Name: SharedAccess
Display Name: Windows Güvenlik Duvarı/Internet Bağlantı Paylaşımı (ICS)
Service Type: shares a process with other services
Service Name: ShellHWDetection
Display Name: Kabuk Donanım Algılaması
Service Type: shares a process with other services
Service Name: srservice
Display Name: Sistem Geri Yükleme Hizmeti
Service Type: shares a process with other services
Service Name: TapiSrv
Display Name: Telefon
Service Type: shares a process with other services
Service Name: Themes
Display Name: Temalar
Service Type: shares a process with other services
Service Name: TrkWks
Display Name: Dağıtılmış Bağlantı İzleme İstemcisi
Service Type: shares a process with other services
Service Name: W32Time
Display Name: Windows Saati
Service Type: shares a process with other services
Service Name: winmgmt
Display Name: Windows Yönetim Yardımcıları
Service Type: shares a process with other services
Service Name: wscsvc
Display Name: Güvenlik Merkezi
Service Type: shares a process with other services
Service Name: wuauserv
Display Name: Otomatik Güncelleştirmeler
Service Type: shares a process with other services
Service Name: WZCSVC
Display Name: Kablosuz Sıfır Yapılandırma
Service Type: shares a process with other services

6) PR-PORTS GÜNLÜK DOSYASI

PR-PORTS günlük dosyası, bilgisayardaki TCP ve UDP bağlantı noktalarındaki etkinlikle ilgili özet verileri içerir. Veriler, aşağıdaki gibi bir virgülle ayrılmış değer (csv) biçimi kullanılarak listelenir:

"date,time,protocol,local port,local IP address,remote port,remote IP address,PID,module,user context"

Bağlantı noktası ile işlem eşleşmelerinin desteklenmediği Windows 2000 tabanlı bilgisayarlarda, Port Reporter hizmeti verileri aşağıdaki biçimi kullanarak listeler:

"date,time,protocol,local port,local IP address,remote port,remote IP address"

Aşağıda örnek bir PR-PORTS günlük dosyasının özeti bulunmaktadır:

Port Reporter Version 1.01 Log File - Port usage log
Check PR-PIDS-09-06-11-13-7-35.log for corresponding process data
Log format:
date,time,protocol,local port,local IP address,remote port,remote IP address,PID,module,user context
(tarih,saat,protokol,yerel bağlantı noktası,yerel IP adresi,uzak bağlantı noktası,uzak IP adresi,PID,modü,kullanıcı bağlamı)
09/6/11,13:07:41,TCP,2034,127.0.0.1,30606,127.0.0.1,3844,firefox.exe,<CLBR-E1614F7672\Clbr.FenTanyL>
09/6/11,13:07:41,TCP,30606,127.0.0.1,2034,127.0.0.1,804,ekrn.exe,<NT AUTHORITY\SYSTEM>
09/6/11,13:07:41,TCP,2035,192.168.2.2,80,85.25.120.145,804,ekrn.exe,<NT AUTHORITY\SYSTEM>
09/6/11,13:07:42,TCP,2036,127.0.0.1,30606,127.0.0.1,3844,firefox.exe,<CLBR-E1614F7672\Clbr.FenTanyL>
09/6/11,13:07:42,TCP,2038,127.0.0.1,30606,127.0.0.1,3844,firefox.exe,<CLBR-E1614F7672\Clbr.FenTanyL>
09/6/11,13:07:42,TCP,30606,127.0.0.1,2036,127.0.0.1,804,ekrn.exe,<NT AUTHORITY\SYSTEM>
09/6/11,13:07:42,TCP,30606,127.0.0.1,2038,127.0.0.1,804,ekrn.exe,<NT AUTHORITY\SYSTEM>
09/6/11,13:07:42,TCP,2037,192.168.2.2,80,85.25.120.145,804,ekrn.exe,<NT AUTHORITY\SYSTEM>
09/6/11,13:07:42,TCP,2039,192.168.2.2,80,85.25.120.145,804,ekrn.exe,<NT AUTHORITY\SYSTEM>
09/6/11,13:08:0,TCP,2040,127.0.0.1,30606,127.0.0.1,3844,firefox.exe,<CLBR-E1614F7672\Clbr.FenTanyL>
09/6/11,13:08:0,TCP,2041,127.0.0.1,80,127.0.0.1,804,ekrn.exe,<NT AUTHORITY\SYSTEM>
09/6/11,13:08:0,TCP,2042,127.0.0.1,30606,127.0.0.1,3844,firefox.exe,<CLBR-E1614F7672\Clbr.FenTanyL>
09/6/11,13:08:1,TCP,2043,127.0.0.1,80,127.0.0.1,804,ekrn.exe,<NT AUTHORITY\SYSTEM>
09/6/11,13:08:1,TCP,2044,127.0.0.1,30606,127.0.0.1,3844,firefox.exe,<CLBR-E1614F7672\Clbr.FenTanyL>
09/6/11,13:08:1,TCP,2045,127.0.0.1,80,127.0.0.1,804,ekrn.exe,<NT AUTHORITY\SYSTEM>
09/6/11,13:08:1,TCP,2046,127.0.0.1,30606,127.0.0.1,3844,firefox.exe,<CLBR-E1614F7672\Clbr.FenTanyL>
09/6/11,13:08:1,TCP,2047,127.0.0.1,80,127.0.0.1,804,ekrn.exe,<NT AUTHORITY\SYSTEM>
09/6/11,13:08:1,TCP,30606,127.0.0.1,2040,127.0.0.1,804,ekrn.exe,<NT AUTHORITY\SYSTEM>
09/6/11,13:08:1,TCP,30606,127.0.0.1,2042,127.0.0.1,804,ekrn.exe,<NT AUTHORITY\SYSTEM>
09/6/11,13:08:1,TCP,30606,127.0.0.1,2044,127.0.0.1,804,ekrn.exe,<NT AUTHORITY\SYSTEM>
09/6/11,13:08:1,TCP,30606,127.0.0.1,2046,127.0.0.1,804,ekrn.exe,<NT AUTHORITY\SYSTEM>
09/6/11,13:08:12,TCP,2054,127.0.0.1,30606,127.0.0.1,3844,firefox.exe,<CLBR-E1614F7672\Clbr.FenTanyL>
09/6/11,13:08:12,TCP,2055,127.0.0.1,80,127.0.0.1,804,ekrn.exe,<NT AUTHORITY\SYSTEM>
09/6/11,13:08:12,TCP,2056,127.0.0.1,30606,127.0.0.1,3844,firefox.exe,<CLBR-E1614F7672\Clbr.FenTanyL>
09/6/11,13:08:12,TCP,2057,127.0.0.1,80,127.0.0.1,804,ekrn.exe,<NT AUTHORITY\SYSTEM>
09/6/11,13:08:12,TCP,30606,127.0.0.1,2054,127.0.0.1,804,ekrn.exe,<NT AUTHORITY\SYSTEM>
09/6/11,13:08:12,TCP,30606,127.0.0.1,2056,127.0.0.1,804,ekrn.exe,<NT AUTHORITY\SYSTEM>
09/6/11,13:08:16,TCP,2060,127.0.0.1,30606,127.0.0.1,3844,firefox.exe,<CLBR-E1614F7672\Clbr.FenTanyL>
09/6/11,13:08:17,TCP,2061,127.0.0.1,80,127.0.0.1,804,ekrn.exe,<NT AUTHORITY\SYSTEM>
09/6/11,13:08:17,TCP,2062,127.0.0.1,30606,127.0.0.1,3844,firefox.exe,<CLBR-E1614F7672\Clbr.FenTanyL>

09/6/11,13:08:17,TCP,2063,127.0.0.1,80,127.0.0.1,804,ekrn.exe,<NT AUTHORITY\SYSTEM>
09/6/11,13:08:17,TCP,2064,127.0.0.1,30606,127.0.0.1,3844,firefox.exe,<CLBR-E1614F7672\Clbr.FenTanyL>
09/6/11,13:08:17,TCP,2065,127.0.0.1,80,127.0.0.1,804,ekrn.exe,<NT AUTHORITY\SYSTEM>
09/6/11,13:08:17,TCP,2066,127.0.0.1,30606,127.0.0.1,3844,firefox.exe,<CLBR-E1614F7672\Clbr.FenTanyL>
09/6/11,13:08:17,TCP,2067,127.0.0.1,80,127.0.0.1,804,ekrn.exe,<NT AUTHORITY\SYSTEM>
09/6/11,13:08:17,TCP,30606,127.0.0.1,2060,127.0.0.1,804,ekrn.exe,<NT AUTHORITY\SYSTEM>
09/6/11,13:08:17,TCP,30606,127.0.0.1,2062,127.0.0.1,804,ekrn.exe,<NT AUTHORITY\SYSTEM>
09/6/11,13:08:17,TCP,30606,127.0.0.1,2064,127.0.0.1,804,ekrn.exe,<NT AUTHORITY\SYSTEM>
09/6/11,13:08:18,TCP,30606,127.0.0.1,2066,127.0.0.1,804,ekrn.exe,<NT AUTHORITY\SYSTEM>
09/6/11,13:08:23,TCP,2068,127.0.0.1,30606,127.0.0.1,3844,firefox.exe,<CLBR-E1614F7672\Clbr.FenTanyL>
09/6/11,13:08:23,TCP,2069,127.0.0.1,30606,127.0.0.1,3844,firefox.exe,<CLBR-E1614F7672\Clbr.FenTanyL>
09/6/11,13:08:23,TCP,2070,127.0.0.1,80,127.0.0.1,804,ekrn.exe,<NT AUTHORITY\SYSTEM>
09/6/11,13:08:23,TCP,2071,127.0.0.1,80,127.0.0.1,804,ekrn.exe,<NT AUTHORITY\SYSTEM>
09/6/11,13:08:23,TCP,2072,127.0.0.1,30606,127.0.0.1,3844,firefox.exe,<CLBR-E1614F7672\Clbr.FenTanyL>
09/6/11,13:08:23,TCP,2073,127.0.0.1,80,127.0.0.1,804,ekrn.exe,<NT AUTHORITY\SYSTEM>
09/6/11,13:08:23,TCP,2074,127.0.0.1,30606,127.0.0.1,3844,firefox.exe,<CLBR-E1614F7672\Clbr.FenTanyL>

7) PR-PIDS GÜNLÜK DOSYASI

PR-PIDS günlük dosyası, bir işlemle ilgili olarak bağlantı noktaları, işlemler, modüller ve işlemin çalışmak için kullandığı kullanıcı hesabı hakkında bilgiler içerir. Aşağıda örnek bir PR-PIDS günlük dosyasının özeti bulunmaktadır:

// Bu örnekte yanlızca Firefox.exe dosyasına bağlı olayların özeti incelenmiştir.
Port Statistics
TCP mappings: 23
UDP mappings: 0
TCP ports in a ESTABLISHED state: 23 = 100.00%
Loaded modules:
// Çalıştırdığımız EXE Dosyası
C:\Program Files\Mozilla Firefox\firefox.exe (0x00400000)
Bu EXE dosyasıyla bağlantılı .dll dosyaları
C:\WINDOWS\system32\ntdll.dll (0x7C8F0000)
C:\WINDOWS\system32\kernel32.dll (0x7C800000)
C:\Program Files\Mozilla Firefox\xul.dll (0x60490000)
C:\Program Files\Mozilla Firefox\sqlite3.dll (0x60210000)
C:\Program Files\Mozilla Firefox\MOZCRT19.dll (0x60000000)
C:\WINDOWS\system32\msvcrt.dll (0x77C00000)
C:\Program Files\Mozilla Firefox\js3250.dll (0x60100000)
C:\Program Files\Mozilla Firefox\nspr4.dll (0x600B0000)
C:\WINDOWS\system32\ADVAPI32.dll (0x77DC0000)
C:\WINDOWS\system32\RPCRT4.dll (0x77E70000)
C:\WINDOWS\system32\Secur32.dll (0x77FE0000)
C:\WINDOWS\system32\WSOCK32.dll (0x71AC0000)
C:\WINDOWS\system32\WS2_32.dll (0x71AA0000)
C:\WINDOWS\system32\WS2HELP.dll (0x71A90000)
C:\WINDOWS\system32\WINMM.dll (0x76B30000)
C:\WINDOWS\system32\USER32.dll (0x7E360000)
C:\WINDOWS\system32\GDI32.dll (0x77F10000)
C:\Program Files\Mozilla Firefox\smime3.dll (0x60430000)
C:\Program Files\Mozilla Firefox\nss3.dll (0x60340000)
C:\Program Files\Mozilla Firefox\nssutil3.dll (0x603F0000)
C:\Program Files\Mozilla Firefox\plc4.dll (0x600F0000)
C:\Program Files\Mozilla Firefox\plds4.dll (0x600E0000)
C:\Program Files\Mozilla Firefox\ssl3.dll (0x60410000)

C:\WINDOWS\system32\SHELL32.dll (0x7C9B0000)
C:\WINDOWS\system32\SHLWAPI.dll (0x77F60000)
C:\WINDOWS\system32\ole32.dll (0x774D0000)
C:\WINDOWS\system32\VERSION.dll (0x77BF0000)
C:\WINDOWS\system32\WINSPOOL.DRV (0x72FD0000)
C:\WINDOWS\system32\COMDLG32.dll (0x76390000)
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03\COMCTL32.dll (0x773C0000)
C:\WINDOWS\system32\IMM32.dll (0x76370000)
C:\WINDOWS\system32\MSIMG32.dll (0x76360000)
C:\WINDOWS\system32\USP10.dll (0x75520000)
C:\WINDOWS\system32\OLEAUT32.dll (0x77110000)
C:\Program Files\Mozilla Firefox\xpcom.dll (0x60E00000)
c:\progra~1\agnitum\outpos~1\wl_hook.dll (0x10000000)
C:\WINDOWS\system32\dbghelp.dll (0x59CA0000)
C:\Program Files\ESET\ESET NOD32 Antivirus\eplgHooks.dll (0x22200000)
C:\WINDOWS\system32\MSCTF.dll (0x746F0000)
C:\WINDOWS\system32\SETUPAPI.dll (0x77910000)
C:\WINDOWS\system32\msctfime.ime (0x75470000)
C:\WINDOWS\system32\CLBCATQ.DLL (0x76FC0000)
C:\WINDOWS\system32\COMRes.dll (0x77040000)
C:\Program Files\Mozilla Firefox\components\browserdirprovider.dll (0x601B0000)
C:\WINDOWS\system32\mswsock.dll (0x71A40000)
C:\WINDOWS\system32\hnetcfg.dll (0x698D0000)
C:\WINDOWS\System32\wshtcpip.dll (0x71A80000)
C:\WINDOWS\system32\iphlpapi.dll (0x76D50000)
C:\WINDOWS\system32\uxtheme.dll (0x5B2A0000)
C:\WINDOWS\system32\DNSAPI.dll (0x76F10000)
C:\WINDOWS\System32\winrnr.dll (0x76FA0000)
C:\WINDOWS\system32\WLDAP32.dll (0x76F50000)
C:\WINDOWS\system32\xpsp2res.dll (0x20000000)
C:\Program Files\Mozilla Firefox\components\brwsrcmp.dll (0x601C0000)
C:\WINDOWS\system32\netapi32.dll (0x6FF90000)
C:\WINDOWS\system32\urlmon.dll (0x61410000)
C:\WINDOWS\system32\iertutil.dll (0x5DCA0000)
C:\Program Files\Mozilla Firefox\extensions\{B13721C7-F507-4982-B2E5-502A71474FED}\components\PNRComponent.dll (0x01E90000)
C:\Program Files\Skype\Toolbars\Shared\SPhoneParser.dll (0x02300000)
C:\Program Files\Mozilla Firefox\softokn3.dll (0x602F0000)
C:\Program Files\Mozilla Firefox\nssdbm3.dll (0x60320000)
C:\Program Files\Mozilla Firefox\freebl3.dll (0x60450000)
C:\Program Files\Mozilla Firefox\nssckbi.dll (0x602A0000)
C:\WINDOWS\system32\rasadhlp.dll (0x76FB0000)
C:\WINDOWS\system32\asycfilt.dll (0x70E90000)
C:\WINDOWS\system32\shdocvw.dll (0x77750000)
C:\WINDOWS\system32\CRYPT32.dll (0x77A70000)
C:\WINDOWS\system32\MSASN1.dll (0x77B10000)
C:\WINDOWS\system32\CRYPTUI.dll (0x754A0000)
C:\WINDOWS\system32\WINTRUST.dll (0x76C20000)
C:\WINDOWS\system32\IMAGEHLP.dll (0x76C80000)
C:\WINDOWS\system32\WININET.dll (0x771B0000)
C:\WINDOWS\system32\Normaliz.dll (0x03540000)
C:\WINDOWS\system32\SXS.DLL (0x75E70000)
C:\WINDOWS\system32\wdmaud.drv (0x72CF0000)
C:\WINDOWS\system32\msacm32.drv (0x72CE0000)
C:\WINDOWS\system32\MSACM32.dll (0x77BD0000)
C:\WINDOWS\system32\midimap.dll (0x77BC0000)
C:\WINDOWS\system32\mscms.dll (0x73B00000)
C:\WINDOWS\system32\icm32.dll (0x63160000)

C:\WINDOWS\system32\appHelp.dll (0x77B30000)
C:\WINDOWS\System32\cscui.dll (0x05CC0000)
C:\WINDOWS\System32\CSCDLL.dll (0x765E0000)
C:\WINDOWS\system32\browseui.dll (0x75F60000)
C:\WINDOWS\system32\USERENV.dll (0x769B0000)
C:\WINDOWS\system32\ntshrui.dll (0x76980000)
C:\WINDOWS\system32\ATL.DLL (0x76B10000)
C:\WINDOWS\system32\LINKINFO.dll (0x76970000)
C:\WINDOWS\system32\Macromed\Flash\NPSWF32.dll (0x09B40000)
C:\WINDOWS\system32\mlang.dll (0x75D80000)
C:\WINDOWS\system32\schannel.dll (0x767E0000)
==========
Log number: 2
Log entry below recorded at: 09/6/11,12:55:16
==========
Process ID: 3844 (firefox.exe)
User context: CLBR-E1614F7672\Clbr.FenTanyL
Process doesn't appear to be a service

PID	Port	Local IP	State	Remote IP:Port
3844	TCP 3929	127.0.0.1	ESTABLISHED	127.0.0.1:3930
3844	TCP 3930	127.0.0.1	ESTABLISHED	127.0.0.1:3929
3844	TCP 3932	127.0.0.1	ESTABLISHED	127.0.0.1:3933
3844	TCP 3933	127.0.0.1	ESTABLISHED	127.0.0.1:3932
3844	TCP 3997	127.0.0.1	ESTABLISHED	127.0.0.1:30606
3844	TCP 4047	127.0.0.1	ESTABLISHED	127.0.0.1:30606
3844	TCP 4057	127.0.0.1	ESTABLISHED	127.0.0.1:30606
3844	TCP 4157	127.0.0.1	ESTABLISHED	127.0.0.1:30606
3844	TCP 4201	127.0.0.1	ESTABLISHED	127.0.0.1:30606
3844	TCP 4203	127.0.0.1	ESTABLISHED	127.0.0.1:30606
3844	TCP 4205	127.0.0.1	ESTABLISHED	127.0.0.1:30606
3844	TCP 4229	127.0.0.1	ESTABLISHED	127.0.0.1:30606
3844	TCP 4231	127.0.0.1	ESTABLISHED	127.0.0.1:30606
3844	TCP 4235	127.0.0.1	ESTABLISHED	127.0.0.1:30606
3844	TCP 4609	127.0.0.1	ESTABLISHED	127.0.0.1:30606
3844	TCP 4611	127.0.0.1	ESTABLISHED	127.0.0.1:30606
3844	TCP 4697	127.0.0.1	ESTABLISHED	127.0.0.1:30606
3844	TCP 4699	127.0.0.1	ESTABLISHED	127.0.0.1:30606
3844	TCP 4709	127.0.0.1	ESTABLISHED	127.0.0.1:30606
3844	TCP 4775	127.0.0.1	ESTABLISHED	127.0.0.1:30606
3844	TCP 4777	127.0.0.1	ESTABLISHED	127.0.0.1:30606
3844	TCP 4779	127.0.0.1	ESTABLISHED	127.0.0.1:30606
3844	TCP 4781	127.0.0.1	ESTABLISHED	127.0.0.1:30606

Bir dahaki yazımda PortQueryUI, Port Reporter Parser araçlarını tanıtacağım. Görüşmek üzere.

REFERANSLAR

http://www.microsoft.com/downloads/details.aspx?familyid=69ba779b-bae9-4243-b9d6-63e62b4bcd2e&displaylang=en
http://support.microsoft.com/kb/837243

MUSTAFA SERHAT DÜNDAR