PENGUMPULAN INFORMASI

Ketika ingin menyelidiki sebuah PC untuk melihat informasi yang terkandung di dalamnya, Anda menggunakan teknik-teknik forensik. Forensik sendiri banyak kegunaannya, selain untuk keperluan penyelidikan kriminalitas -sebagaimana yang banyak terjadi di ranah hukum cybercrime oleh para petugas-, juga banyak dilakukan oleh para hacker untuk mengetahui serta mencari atau mencuri informasi dari sebuah komputer. Apa pun tujuannya, komputer forensik merupakan sebuah ilmu yang sangat menarik untuk dipelajari.

1.1 Pengenalan

Apakah *Computer Forensic* itu? Computer forensic atau forensik komputer, yaitu sebuah proses investigasi peranti komputer atau peranti simpannya, baik berupa komputer pribadi, laptop, server, PC kantoran, atau media *removable* untuk menentukan apakah komputer atau peralatan ini digunakan untuk keperluan yang ilegal, tidak sah, atau tidak biasa.

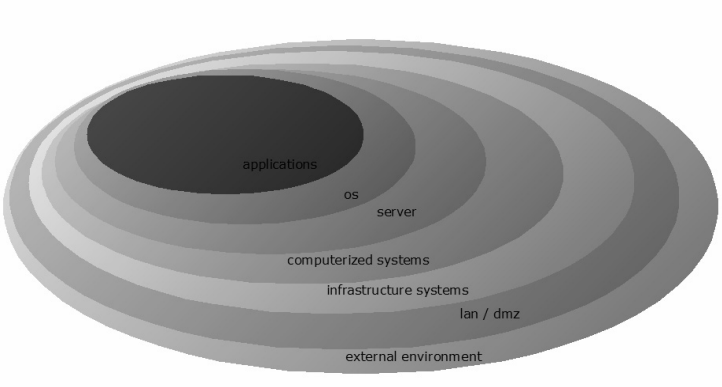
Forensik juga bisa mencakup monitoring jaringan komputer untuk keperluan yang sama.

Jadi, pada prinsipnya kegiatan forensik ini merupakan bagian dari hacking, di mana kalau hacking serius, nantinya ditindaklanjuti dengan pemindaian vulnerability dan eksploitasi.

Computer forensic terdiri atas berbagai aspek tahapan berikut:

1. Identify evidence (mengidentifikasi bukti)
2. Preserve evidence (memelihara bukti)
3. Analyze evidence (menganalisis bukti)
4. Present results (mempresentasikan hasil)

Tahapan-tahapan ini perlu menggunakan metode yang terstandardisasi, terutama kalau diperlukan dalam lingkup hukum.



Gambar 1.1 Cakupan forensik komputer, tugasnya adalah menyediakan data

Saat ini, mulai lazim kegiatan pengumpulan informasi pada tahapan forensik komputer dilakukan dari saat komputer masih berjalan. Ini karena pendekatan forensik klasik sudah dianggap tidak relevan lagi untuk dunia modern, di mana penyelidik mematikan komputer, dan kemudian mengambil hard disk-nya dan memproses hard disk untuk memperoleh gambaran *bit-stream*-nya.

Padahal banyak informasi yang tidak dapat diambil hanya dari hard disk saja. Misalnya data Instant Messaging (IM), yang biasanya tidak tersimpan ke hard disk.

Dalam banyak kasus, informasi yang paling berharga kadang justru yang tersedia di memori komputer, yang artinya hanya bisa diakses ketika komputer masih berjalan. Termasuk dari cakupan memori komputer di sini adalah: koneksi jaringan, konten dari software IM client, memori yang digunakan oleh program (misalnya IM). Untuk itulah diperlukan *live response* atau pengumpulan data secara live ketika komputer masih menyala.

1.2 Pengumpulan Informasi secara Live

Penyelidik forensik kadang tidak bisa mematikan PC karena PC tersebut memang harus selalu menyala saat layanannya diperlukan. Misalnya pada komputer yang menjadi server e-commerce. Di mana kalau ada downtime, maka kerugiannya bisa dihitung dengan uang.

Internet yang merupakan dunia tanpa batas, kini tidak hanya banyak dimanfaatkan oleh masyarakat awam untuk menikmati informasi, namun juga dimanfaatkan oleh para pelaku kejahatan untuk melakukan aksi kejahatannya. Bahkan katanya, kejahatan di cyberspace ini menghasilkan kerugian finansial yang lebih bahaya dibandingkan dengan kejahatan biasa.

Sama halnya kejahatan di dunia fisik, kejahatan di cyberspace pun makin berkembang. Aktivitas kriminal atau ilegal berkaitan dengan komputer makin hari makin canggih.

Banyak sekali software yang dikembangkan untuk bisa mengambil informasi, mencari kerentanan/vulnerability, kemudian mengeksploitasi kerentanan tersebut. Bahkan ada distro Linux khusus seperti Backtrack

yang bisa digunakan untuk melakukan pengumpulan informasi, pemindaian kerentanan yang ada di komputer, hingga menyetel payload serta pengeksekusian program yang bisa digunakan untuk banyak hal, termasuk pencurian data. Misalnya data password, username, file pribadi, pencurian data kartu kredit, pengumpulan alamat email untuk spamming, dan sebagainya.

Pencarian informasi secara live ini juga bisa dijadikan pendahuluan untuk kemudian melanjutkannya dengan melakukan pencarian secara offline, ketika komputer dimatikan nanti.

Kebanyakan informasi yang dikumpulkan ketika komputer masih hidup adalah informasi yang sifatnya **volatil**, yaitu informasi yang hilang kalau komputer dihidupkan.

Yang termasuk data volatil ini adalah:

- Register, isi cache.
- Memori.
- Koneksi jaringan.
- Proses yang sedang berjalan.

Informasi volatil ini biasanya ada di memori fisik (RAM) dan terdiri atas informasi mengenai:

- Proses yang ada di komputer.
- Isi clipboard.
- Dan lain sebagainya.

Informasi-informasi ini biasanya menjelaskan tentang kondisi sistem saat itu. Hacker atau penyelidik yang ingin menyelidiki kejadian pada saat masih fresh harus mengumpulkan informasi ini dengan secepatnya

menangkap dan menganalisis data, di mana caranya akan dijelaskan di tahap selanjutnya.

Penganalisisan data bisa digunakan untuk melihat sifat dan cakupan dari sebuah kejadian yang akan diselidiki dengan ilmu forensik ini. Ketika kabel listrik dicabut, dan komputer dimatikan, maka informasi volatil ini otomatis akan hilang.

Ada banyak tool yang bisa digunakan untuk mengumpulkan informasi volatil dari sistem yang live. Sehingga hacker/penyelidik bisa mendapatkan gambaran keseluruhan yang lebih lengkap mengenai kondisi sistem dan juga memberi informasi dalam cakupan yang lebih besar. Inilah yang disebut *respons live*, yaitu mengakses sistem yang sedang berjalan secara live dan mengumpulkan informasi yang volatil atau bukan volatil.

Selain merespons secara live, ada pula istilah lain seperti akuisisi secara live. Apa bedanya? Respons secara live berkaitan dengan pengumpulan informasi volatil dari sistem. Sementara akuisisi live berkaitan dengan pengambilan hard disk ketika sistem sedang berjalan, dengan cara mengambil *image* dari hard disk.

Di bab ini, akan dijelaskan tool, teknik, dan metodologi untuk melakukan pengambilan informasi secara live ini. Kita harus tahu dulu apa yang akan dikumpulkan dan bagaimana mengumpulkannya.

Tapi perlu diketahui terlebih dahulu bahwa ketika melakukan respons live untuk mengumpulkan informasi, kita perlu terlebih dahulu memahami *prinsip Locard*. Yaitu ketika ada dua benda yang bersentuhan (seperti software untuk pengumpulan data dan komputer), maka akan ada transfer proses di antara kedua benda tersebut.

Jadi, ketika investigator sedang menyelidiki di PC, maka software yang dipakai untuk menyelidiki PC tersebut bisa memengaruhi program dan

kondisi komputer yang akan diselidiki. Begitu juga ketika Anda menancapkan peranti seperti flash drive atau Android ke komputer, maka ini akan memengaruhi kondisi di komputer. Perubahan ini bisa bersifat sementara (seperti di proses memori dan jaringan) atau secara permanen (berupa file log dan entri registri).

Program yang dipakai untuk mengumpulkan informasi memiliki efek lain di sistem yang sedang berjalan. Windows melakukan prefetch aplikasi yang akan mengambil informasi mengenai sistem, akses terakhir, dan waktu modifikasi konten file. Jadi, ketika Anda menjalankan program, file prefetch baru akan ditampilkan.

Anda harus tahu mana efek yang disebabkan oleh perilaku Anda saat melakukan forensik dan bukannya kondisi asli dari komputer yang akan diselidiki. Misalnya bisa membedakan isi file .pf (prefetch) yang diakibatkan oleh kita, atau kondisi aslinya.

Dengan memahami ini, Anda bisa memahami tool dengan lebih baik dan bisa mengoptimalkan hasilnya.

Sementara memori non volatil, biasanya terdiri atas:

- Isi dari sistem file dan drive.
- Isi dari removable media.

1.3 Data Apa yang Dikumpulkan

Ketika melakukan pengumpulan data secara live, Anda perlu menentukan apa saja data yang hendak dikumpulkan. Berikut ini beberapa informasi yang biasa dikumpulkan dari pengumpulan data secara live:

- Waktu sistem.
- User yang ter-login.

- File yang dibuka.
- Informasi jaringan.
- Koneksi jaringan.
- Informasi proses.
- Mapping proses ke port.
- Memori proses.
- Status jaringan.
- Isi clipboard.
- Informasi service/driver.
- History dari command.
- Drive yang di-mapping.
- Folder atau file yang di-share.

Untuk tiap tipe dari informasi ini, ada tool-tool sendiri untuk menggunakannya. Kebanyakan tool yang bisa Anda cari di internet untuk keperluan pengumpulan informasi volatil ini adalah yang berbasis command line (CLI). Ini karena peranti yang berbasis command line biasanya memiliki jejak di memori yang lebih kecil. Artinya konsumsi memorinya lebih sedikit, selain itu hanya sedikit menggunakan file DLL dan memiliki pengaruh ke sistem yang lebih kecil.

Alasan lain menggunakan tool berbasis command line adalah karena kepraktisannya dan sangat simpel. Program CLI memiliki satu fungsi khusus dan lebih mudah diotomatisasikan melalui file script. Program berbasis CLI juga bisa dijalankan secara berbarengan menggunakan file batch atau bahasa scripting. Outputnya biasanya dikirim ke konsol dan bisa diarahkan ke file atau ke soket.

Tapi bukan berarti program berbasis grafis (GUI) tidak bisa digunakan untuk melakukan pengumpulan data secara live. Kalau ada, Anda bisa menggunakannya.

Untuk itu minimal Anda perlu menggunakan toolset berupa sebuah CD-ROM, di mana di dalamnya terdapat toolset seperti berikut:

- Versi terpercaya CMD.EXE dari sistem operasi yang sama.
- Netcat atau cryptcat.
- System tool (ipconfig, netstat, date, time, net, arp) untuk berbagai sistem operasi Windows dan level service pack.
- Pstools, listdlls, filemon, regmon, autoruns.
- Hfind, fport, ntlast.
- Windows resource kit tools.
- Sniffer (ethereal, windump).
- Md5sum/md5deep.

Setup yang harus dilakukan adalah:

1. Konek workstation forensik ke LAN yang sama dengan server yang diinvestigasi.
2. Konfigurasikan netcat atau cryptcat di workstation forensik untuk listen ke port tertentu dan menyimpan data yang diterima ke file bukti.
3. Mount toolset dari CD Rom ke server yang dicurigai.
4. Buka konsol yang terpercaya (cmd.exe).

Gambar 1.2 Cara kerja komputer penyelidik (forensic workstation) dengan komputer server yang diselidiki (suspect server)

Di antara tool untuk mendapatkan data volatil adalah:

- date /t & time /t

  Mendapatkan tanggal dan waktu sistem.

- ipconfig /all

  Mendapatkan konfigurasi TCP/IP.

- netstat –aon

  Mendapatkan koneksi jaringan dan port listening (dengan PID proses akan ditampilkan).

- psinfo –shd

  Mendapatkan informasi komputer (hardware, software, hotfixe, version, dan sebagainya).

- pslist –t

  Mendapatkan proses yang running.

- at

  Mendapatkan task yang dijadwalkan (cek juga pada %windir%\ tasks\folder).

- streams -s c:\

  Menampilkan semua file dengan data stream alternatif.

- logonsessions –p

  Menampilkan semua sesi login dan proses yang berjalan di tiap session.

- arp –a

  Menampilkan cache tabel arp.

- ntlast

  Merekam login yang sukses dan gagal, termasuk session null dan remote login.

- route print

  Menampilkan tabel routing IP.

- autorunsc

  Menampilkan semua item autorun.

- hfind c:

  Mencari file hidden.

- promiscdetect

  Mendeteksi kartu jaringan di mode 'promisc'.

- volume_dump

  Dump informasi mengenai volume, mount, mount point, filesystem, dan seterusnya.

- pwdump2

  Dump nthash/lmhash dari akun lokal untuk cracking.

- lsadump2

  Dump konten dari LSA secret (memerlukan SeDebugPrivilege).

- strings

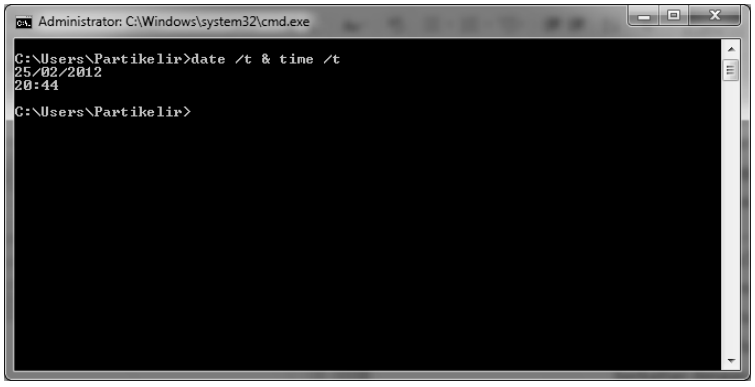
  Mencari string ASCII/unicode di file yang dicurigai.

1.3.1 Mengetahui Waktu Sistem

Informasi pertama yang perlu Anda kumpulkan dari komputer adalah mencatat waktu kapan Anda melakukan investigasi. Ini akan memberikan informasi mengenai konteks dari penyelidikan, karena berkaitan dengan rentang waktu dari kejadian-kejadian yang diselidiki.

Gunakan perintah berikut untuk mengetahui waktu sekarang menurut komputer:

```
> date /t & time /t
```



Gambar 1.3 System time

Tidak hanya system time yang penting, tapi juga uptime alias waktu komputer sudah dinyalakan. Misalnya waktu sebuah proses sudah dijalankan bisa memberikan informasi berharga.

Informasi lainnya adalah zona waktu dari komputer. Sistem Windows yang menggunakan file sistem NTFS menyimpan file time di format UTC. Sementara yang menggunakan sistem file FAT akan menyimpan file time

di sistem file lokal. Ini sangat penting dalam analisis post–mortem yang akan dijelaskan di bagian belakang nantinya.

1.3.2 Mengetahui User yang Login dengan PsLoggedOn

Ketika Anda sedang melakukan forensik pada sebuah komputer, Anda harus tahu siapa saja yang login pada saat kejadian/pada saat sistem sedang live.

Anda bisa mencari tahu siapa yang menggunakan sumber daya (resources) di komputer lokal menggunakan command “net session”. Tapi tidak ada metode built-in di Windows untuk mencari tahu siapa yang menggunakan resource di komputer remote.

Windows NT juga tidak memiliki tool untuk melihat siapa yang login ke komputer, baik secara lokal atau remote. Untuk itu Anda bisa menggunakan PsLoggedOn dari sysinternals.com.

PsLoggedOn adalah sebuah applet yang menampilkan user yang login, baik di komputer user yang login secara lokal, atau via resource untuk komputer lokal atau remote. Jika Anda menentukan nama user dan bukan komputer, maka PsLoggedOn akan mencari komputer di network neighborhood dan memberitahukan jika user tersebut sedang login atau tidak.

Software PsloggedOn disediakan oleh systinternals, bisa diambil dari url http://technet.microsoft.com/en-us/sysinternals/bb897545.

Definisi dari PsLoggedOn tentang user yang login adalah yang profile-nya ter-load di registry. Jadi, program PsLoggedOn menentukan siapa yang login dengan memindai key HKEY_USERS di registry.

Untuk tiap key yang memiliki nama berupa SID (security Identifier), PsLoggedOn akan melihat username yang bersangkutan dan menampilkannya. Untuk menentukan siapa yang login melalui share resource, PsLoggedOn menggunakan NetSessionEnum API.

Untuk menginstal PsLoggedOn, Anda tinggal men-download-nya dari URL yang ada, kemudian menyalinkan file executable dan mengetikkan "psloggedon".

Atau sintaks lengkapnya adalah:

```
psloggedon [- ] [-l] [-x] [\\nama_komputer| username]
```

Beberapa penjelasan dari opsi di atas adalah:

- -

  Menampilkan opsi yang didukung dan satuan pengukuran yang dipakai untuk nilai output.

- -l

  Menampilkan logon lokal saja, dan bukannya logon untuk lokal dan di resource jaringan.

- -x

  Tidak menampilkan waktu logon.

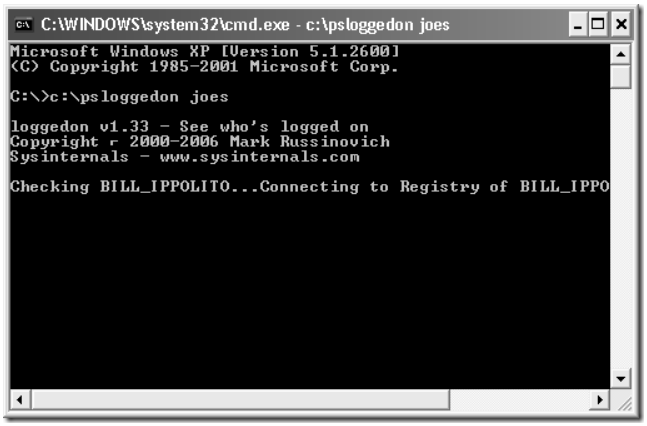
- \\nama_komputer

  Menentukan nama dari komputer di mana informasi logon ditampilkan.

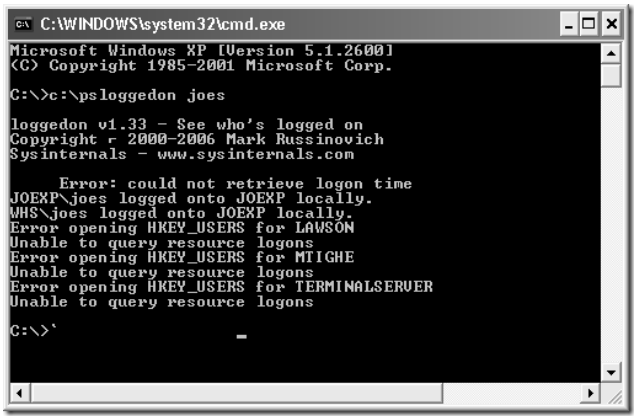
- username

  Jika Anda menentukan username, maka PsLoggedOn mencari komputer di jaringan di mana user ini login. Ini dapat dipakai

untuk memastikan bahwa user tertentu tidak login ketika Anda ingin mengubah konfigurasi profile user-nya.



Gambar 1.4 Penggunaan PSLoggedOn

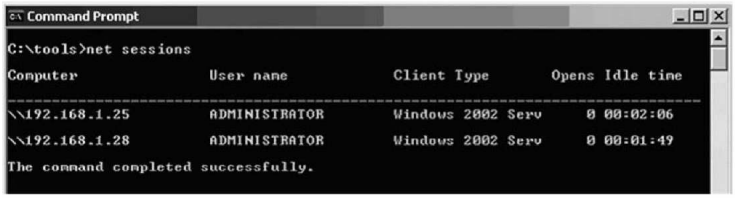


Gambar 1.5 Hasil dari PsLoggedOn

1.3.3 Mencari Session dengan Net Sessions

Command Net Sessions bisa digunakan tidak hanya untuk melihat username yang dipakai untuk mengakses sistem via remote login, tapi

juga bisa digunakan untuk mencari tahu dari mana mereka mengakses sistem. Ini sudah ada di Windows langsung.



Gambar 1.6 Contoh output dari Net Sessions

Anda juga bisa menggunakan perintah "net session" atau "net sess" untuk menjalankan net sessions. Sintaks untuk net session adalah:

```
net session [\\nama_komputer] [/delete]
```

Keterangan dari parameter adalah:

- \\nama_komputer

  Mencari komputer yang akan ditampilkan session-nya atau memiliki session yang diskonek.

- /delete

  Mengakhiri sesi komputer dari nama_komputer dan membuka semua file di komputer untuk session. Jika Anda menghilangkan nama_komputer, maka semua session di komputer.

- net help command

  Menampilkan bantuan untuk command net tertentu.

Menggunakan net session ini bisa mengakibatkan kehilangan data. Anda perlu memperingatkan user sebelum melakukan diskonek pada session.

Net session bisa melihat nama komputer dan nama user yang ada di server. Selain itu, ada pula informasi apa saja file yang dibuka oleh user dan berapa lama session dari user sudah idle.

Contoh informasi yang muncul akan sesuai seperti format berikut:

```
Computer User name Client type Opens Idle time
-------------------------------------------------------------
\\CANDRA    CANDRA   Windows 2000 1 00:00:13
\\SHABILA   Administrator DOS LM 2.1 0 01:05:13
```

Untuk menampilkan session dari user tertentu, gunakan nama_komputer di command. Informasi mengenai user tertentu biasanya termasuk resource yang di-share yang punya koneksi ke user.

Session biasanya direkam ketika user di client sukses mengkontak server. Session dianggap dimulai ketika ada dua komputer di jaringan yang sama, yang memiliki username dan password yang diterima oleh server.

Sebuah user di client harus memiliki session di server sebelum bisa menggunakan resource dari server tersebut. Dan session ini tidak akan ada, sebelum user di client terhubung ke resource. Sebuah client dan server hanya memiliki satu session. Tapi bisa memiliki banyak *entry point*, koneksi, atau resource.

Untuk mengeset berapa banyak session bisa idle sebelum otomatis diskonek, Anda bisa mengeset fitur autodisconnect menggunakan:

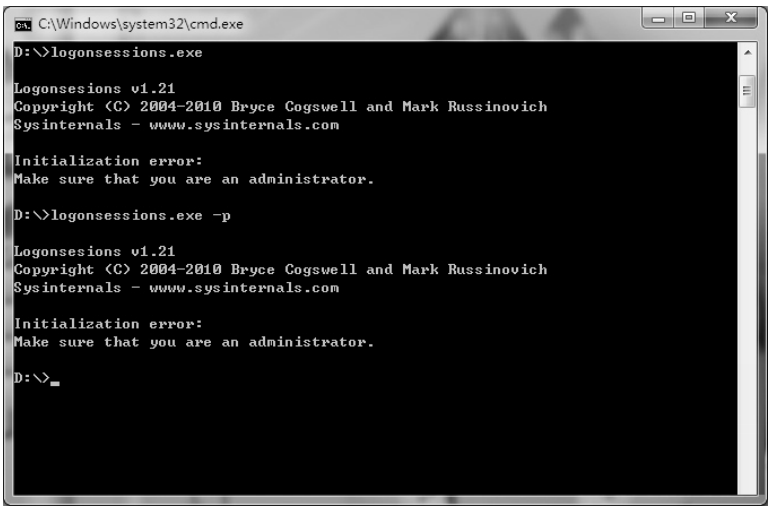
```
net config server /autodisconnect
```

Diskonek otomatis akan terlihat oleh user karena session otomatis melakukan koneksi ulang ketika user mengakses resource lagi. Untuk mengakhiri session di server, gunakan:

```
net session \\nama_komputer /delete.
```

1.3.4 Menampilkan Sesi Login dengan LogonSessions

LoggonSessions mirip dengan tool di atas, ini adalah tool CLI dari sysinternals.com milik Microsoft. Tujuannya adalah mencantumkan semua sesi login aktif di sistem. Software ini bisa diambil dari http://technet.microsoft.com/en-us/sysinternals/bb896769.aspx.



Gambar 1.7 Contoh penggunaan LogonSessions

Untuk mengoperasikannya, gunakan perintah seperti berikut:

```
logonsessions [-p]
```

Tool lain yang bisa digunakan adalah netusers.exe, yaitu tool gratisan dari Somarsoft.com. Dengan menggunakan parameter –local dan–history, Anda bisa men-switch untuk mengambil laporan ringkas dari waktu terakhir semua user login ke sistem. Waktu logon terakhir ini disimpan di registry. Netusers.exe memungkinkan Anda mengambil informasi ini dari sistem live.

Tapi tool-tool ini tidak akan menunjukkan apakah seseorang login via backdoor. Backdoor dan trojan memungkinkan user untuk “login” via trojan atau melalui koneksi TCP/IP dan melewati mekanisme Windows authentication.

Jika output dari psloggedon.exe menunjukkan bahwa user login ke sistem secara remote, Anda bisa melihat file-file yang dibukanya. Biasanya ketika seseorang login secara remote, ia akan mencari informasi tertentu dan membuka file-file.

User di lingkungan korporat bisa men-share file kemudian mengizinkan user lain untuk melihat image, download audio, dan sebagainya.

Bahkan sistem Windows yang terkoneksi ke internet dengan tanpa password administrator dan firewall bisa dikunjungi oleh orang lain secara anonim dan kemudian dicari data-data di dalamnya dan disalin.

Ada program psfile.exe (http://technet.microsoft.com/en-us/sysinternals/bb896649.aspx) dan openfiles.exe (native di Windows XP Pro dan Windows 2003), yang memungkinkan Anda mencari tahu file-file yang dibuka di sistem melalui koneksi remote.

1.3.5 Mencari Informasi Network (Name Table dari Cached NetBIOS)

Ketika orang masuk dan memperoleh akses remote ke sistem, mereka akan mencari tahu apakah ada sistem lain di jaringan dan bisa dilihat oleh sistem.

Kadang file batch sudah dibuat di sistem dan dieksekusi. Sering kali penyusup juga telah me-launch net view melalui sql injection, di mana memasukkannya via browser untuk mengirim command ke sistem melalui web dan server database.

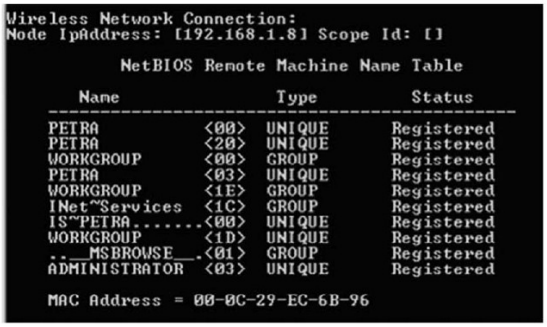
Ketika koneksi dibuat ke sistem lain menggunakan komunikasi NetBios, maka sistem akan me-maintain list dari sistem lain yang dilihat. Dengan melihat konten dari name table yang di-cache, Anda bisa menentukan sistem lain yang sudah terpengaruh.

Misalnya ada sebuah komputer dengan komputer lain di jaringan yang menggunakan konfigurasi DHCP (*Dynamic Host Configuration Protocol*). Di komputer Windows, pertama, diketikkan nbtstat -A 192.168.1.22 untuk melihat name table dari komputer remote. Kemudian mengetikkan nbtstat -c untuk melihat cache NetBIOS di sistem operasi host.

Gambar 1.8 Melihat name table

Bagaimana memanfaatkan data ini? Biasanya ketika seorang penyerang memiliki akses ke sistem, maka ia akan tertarik untuk mendapatkan akses ke sistem lain juga. Untuk melakukan ini, ia harus mencari tahu sistem apa saja yang ada di jaringan dan kelemahan apa yang dimiliki.

Salah satu tool untuk mengetahui kelemahan sistem adalah nbstat. Berikut ini contoh output dari command nbstat untuk mengisikan nama cache netBIOS.



Gambar 1.9 Output dari nbstat –A host

Dari output di atas, kita bisa tahu bahwa admin sedang login dan server jalan menggunakan webserver *Internet Information Server* (IIS). *Penetration Tester* dan penyerang biasanya menggunakan informasi di name table dari NETBIOS di semua sistem yang bisa dikompromikan. Untuk menenentukan lokasi vulnerabilitas sistem, Anda bisa melihat informasi dari artikel Microsoft Knowledge Base 163409 (http://support.microsoft.com/kb/q163409) dan 119495 (http://support.microsoft.com/kb/119495/EN-US).

Setelah sebuah insiden dilaporkan, penyelidik forensik biasanya langsung mengumpulkan informasi mengenai koneksi jaringan ke dan dari sistem yang terpengaruh.

Informasi ini bisa kedaluwarsa. Dan jika terlalu lama, ini bahkan bisa hilang. Seorang investigator biasa melihat apakah penyerang masih login dan mengakses sistem. Atau bisa juga menggunakan worm atau bot IRC sehingga bisa berkomunikasi keluar dari sistem.

Investigator bisa menyelidiki bagaimana kondisi sistem, apakah tetap, meng-update dirinya sendiri, atau login ke server command dan control. Informasi ini bisa menyediakan petunjuk penting dan konteks lainnya ke informasi yang sudah dikumpulkan oleh investigator.

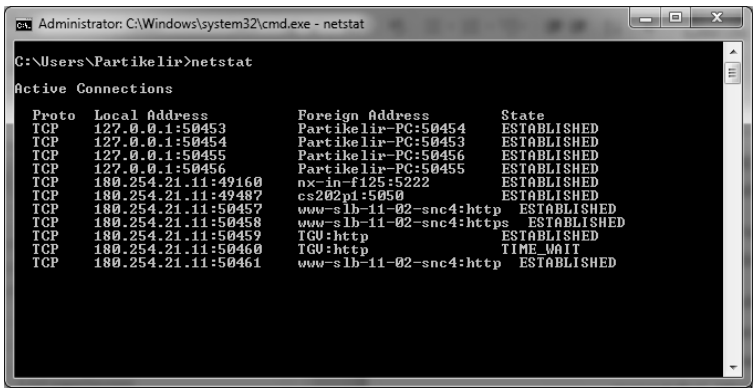
Tidak semua sistem memiliki firewall yang terinstal. Anda bisa menggunakan aplikasi seperti Port Reporter (http://support.microsoft.com/kb/837243) untuk merekam dan mencatat koneksi log jaringan.

Investigator harus bisa bereaksi dengan cepat dan mengumpulkan semua informasi yang dibutuhkan dengan efisien dan dengan waktu yang singkat.

1.3.6 Pengumpulan Informasi dengan Netstat

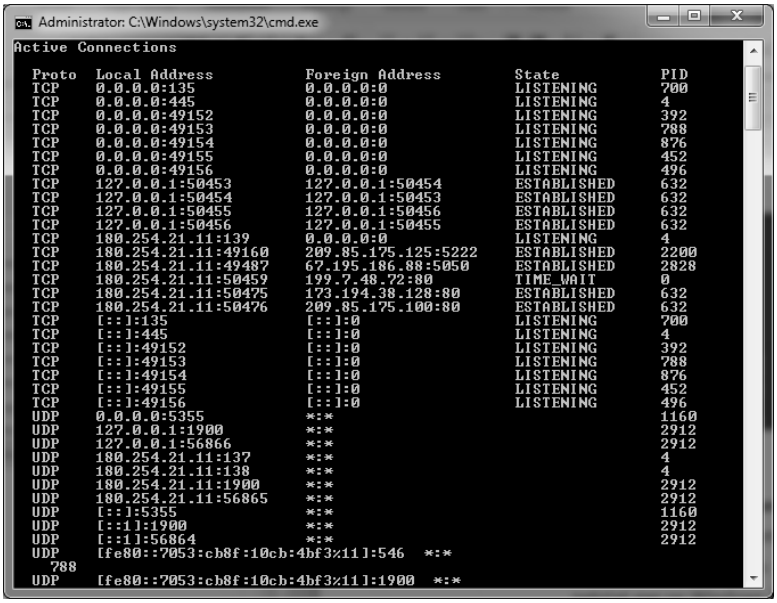
Netstat termasuk salah satu tool paling terkenal untuk mengumpulkan informasi di jaringan Windows. Tool netstat.exe merupakan tool berbasis CLI, yang gunanya untuk melihat koneksi TCP dan UDP serta kondisinya, statistik jaringannya, dan sebagainya.

Netstat.exe merupakan tool native, artinya merupakan bagian dari sistem operasi Windows.



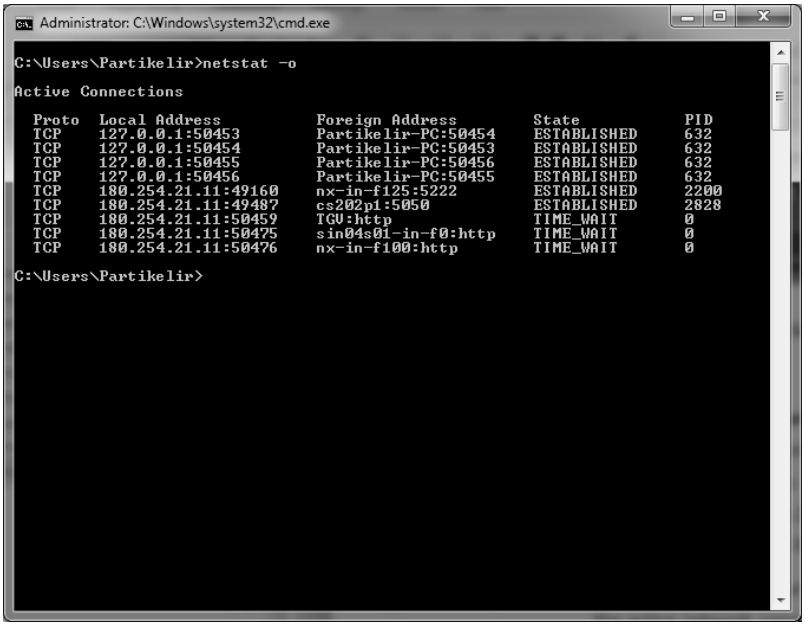
Gambar 1.10 Penggunaan Netstat.exe tanpa parameter tambahan

Salah satu metode penting untuk menjalankan netstat adalah dengan menggunakan parameter –ano. Ini akan memerintahkan program untuk menampilkan koneksi jaringan TCP dan UDP, listening ke port, dan mengetahui identifier dari proses (PID)-nya menggunakan koneksi jaringan tersebut.



Gambar 1.11 Contoh netstat ano

Dalam kondisi normal, Windows 2000 tidak merespons parameter –o ketika menjalankan netstat.exe. Namun, ada hotfix yang memungkinkan versi netstat.exe di Windows 2000 untuk menampilkan PID untuk proses yang memiliki koneksi jaringan yang ditampilkan di output.



Gambar 1.12 Perintah netstat -o

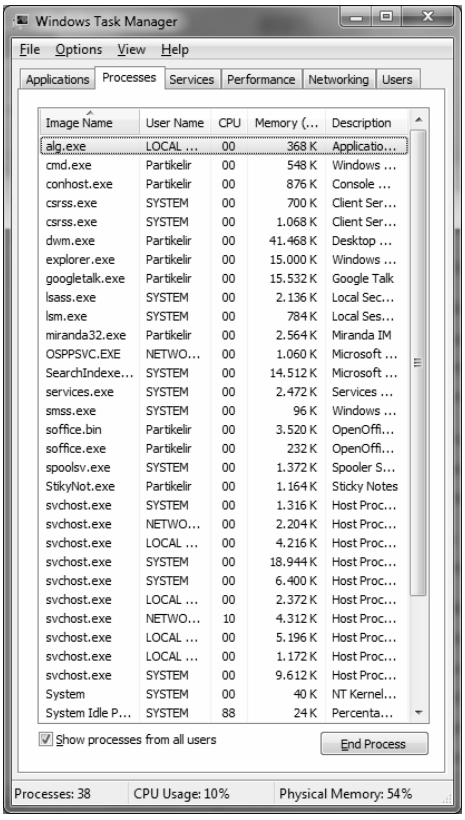
Output dari netstat -ano akan menampilkan koneksi jaringan aktif, kondisi dari tiap koneksi, dan PID dari proses yang menggunakan port. Ketika Anda melihat output dari netstat, bahwa ada koneksi yang tidak biasa, misalnya koneksi dari port 80, maka PID dari proses yang memakai koneksi ini akan me-map kembali ke web browser.

Misalnya ada program yang konek ke sistem remote kemudian menjalankan wget.exe di Windows untuk men-download file malware. Karena ini akan terlihat di software IDS sebagai aplikasi web normal.

Menggunakan netstat dengan parameter –r akan menampilkan tabel routing dan menentukan apakah routing tertentu diaktifkan di sistem. Ini akan menampilkan berbagai informasi yang sangat penting ke investigator.

1.3.7 Mencari Informasi tentang Proses

Investigator akan berusaha mencari tahu proses yang berjalan di sistem. Ketika Anda melihat **Processes** di **Windows Task manager**, Anda bisa melihat informasi mengenai tiap proses.



Gambar 1.13 Task Manager

Tapi untuk kegiatan forensik, Anda perlu mencari tahu banyak info lainnya seputar proses yang tidak terlihat di Task Manager, antara lain:

- Path lengkap dari file .exe-nya.
- Command line yang digunakan untuk menjalankan proses, jika ada.
- Lama waktu di mana proses sudah running.
- Konteks security/user di mana proses dijalankan.
- Modul yang di-load oleh proses.
- Isi memori dari proses.

Task Manager akan berisi sebagian dari informasi ini, tapi tidak lengkap. Misalnya, ada malware yang bisa menginstal dirinya sendiri dan menggunakan nama svchost.exe yang merupakan nama dari proses normal di Windows.

File asli dari svchost.exe ini terletak di direktori system32. Jadi, kalau ada file svchost.exe yang jalan di luar direktori ini, berarti malware.

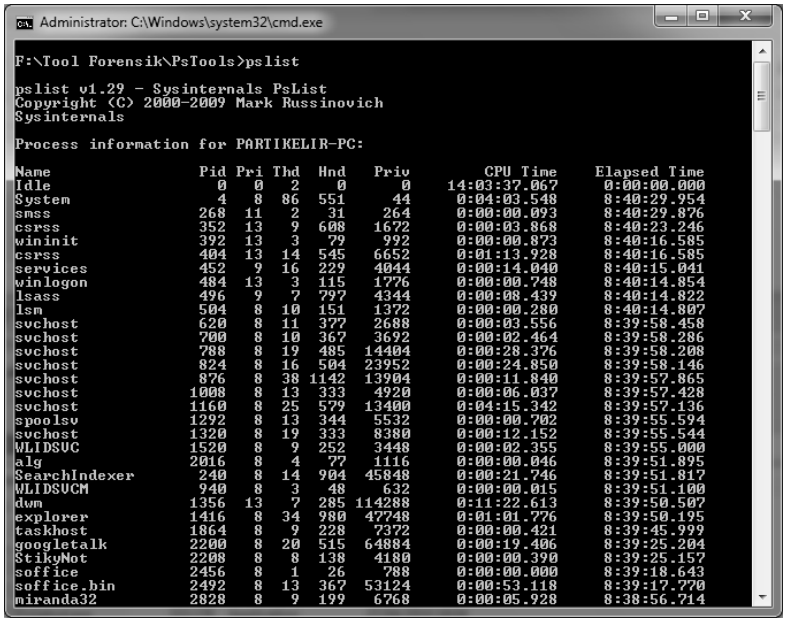
Jika Anda melihat daftar proses di Task Manager, bagaimana cara mengetahui proses tertentu terlihat mencurigakan? Caranya dengan melihat path penuh dari file executable-nya.

Contohnya file svchost.exe di atas, jika berjalan dari selain C:\Windows\system32 maka perlu dicurigai. Begitu juga dengan command line yang digunakan untuk menjalankan proses. Misalnya kalau file inetinfo.exe yang dijalankan dengan argumen —L -d -p 80 —e di cmd.exe harus diwaspadai.

Command ini mengindikasikan penggunaan netcat sebagai backdoor. Banyak malware yang menyamar menggunakan nama-nama dari file yang normal. Misalnya worm W32/Nachi meletakkan salinan utility File

Transfer Protocol (TFTP) di C:\Windows\system32\Wins dan menamainya svchost. exe. Ketika program ini dijalankan, maka user akan mengiranya merupakan program resmi dari svchost.exe.

Anda bisa menggunakan pslist.exe untuk mencari tahu proses yang berjalan via CLI.



Gambar 1.14 Proses yang berjalan diketahui via Process List

Cara kerjanya menggunakan tool PerfMon. PsList menggunakan performance counter untuk memperoleh informasi yang akan ditampilkan. Beberapa penjelasan parameter dari tool ini:

- -d

  Menampilkan detail thread.

- -m

  Menampilkan detail memori.

- -x

  Menampilkan proses, informasi memori, dan thread.

- -t

  Menunjukkan tree dari proses.

- -s [n]

  Menjalankan di mode task manager. Untuk opsi kedua yang ditentukan, pilih Escape untuk membatalkan.

- -r n:

  Mode refresh rate dari Task manager dalam satuan detik.

- \\computer

  Pslist tidak akan menampilkan informasi untuk sistem lokal, tapi untuk komputer tertentu. Anda bisa menggunakan parameter -u dengan username dan password untuk login ke sistem remote.

- -u username

  Username tertentu jika Anda ingin mematikan proses di sistem remote dan akun yang Anda eksekusi tidak punya privilege tertentu.

- -p password

  Opsi ini memungkinkan Anda mengatur info password untuk login di command line sehingga Anda bisa menggunakan PsList dari file batch. Jika Anda menentukan nama akun dan menghilangkan opsi –p, maka pslist akan menanyakan password secara manual.

- name

  Menampilkan info tentang proses yang dimulai dengan name yang ditentukan.

- -e

  Nama pasti dari nama proses.

- pid

  Bukannya menampilkan semua proses yang sedang berjalan, parameter ini akan menampilkan proses yang memiliki PID tertentu saja. Misalnya “pslist 53” akan menampilkan statistik dump untuk proses dengan PID = 53.

1.3.8 Mengetahui Sistem Informasi Lokal & Remote yang Berjalan dengan PSInfo

PsInfo adalah tool command-line untuk mengumpulkan informasi kunci tentang sistem Windows, baik lokal atau remote. Termasuk di antaranya tipe instalasi, build kernel, registered organization dan owner, jumlah prosesor dan tipe, jumlah memori fisik, tanggal instalasi, versi trial, dan tanggal expiration kalau ada.

Berikut ini penggunaan psinfo:

```
psinfo [[\\computer[,computer[,..] | @file [-u user[-p
psswd]]] [-h] [-s] [-d] [-c [-t delimiter]] [filter]
```

Berikut ini penjelasan dari beberapa parameter yang bisa dipakai:

- \\computer

  Menerapkan command di komputer remote atau komputer yang ditentukan. Jika Anda menghilangkan nama komputer, maka command akan dijalankan di komputer lokal. Jika Anda menggunakan tanda bintang sebagai wildcard (*) maka

command hanya berjalan di semua komputer yang ada di domain sekarang.

- @file

  Menjalankan command di tiap komputer yang ditampilkan di file teks yang ditentukan.

- -u

  Menentukan user name opsional untuk login ke komputer remote.

- -p

  Menentukan password opsional untuk username.

- -h

  Menampilkan daftar hotfix yang terinstal.

- -s

  Menampilkan daftar aplikasi terinstal.

- -d

  Menampilkan informasi volume disk.

- -c

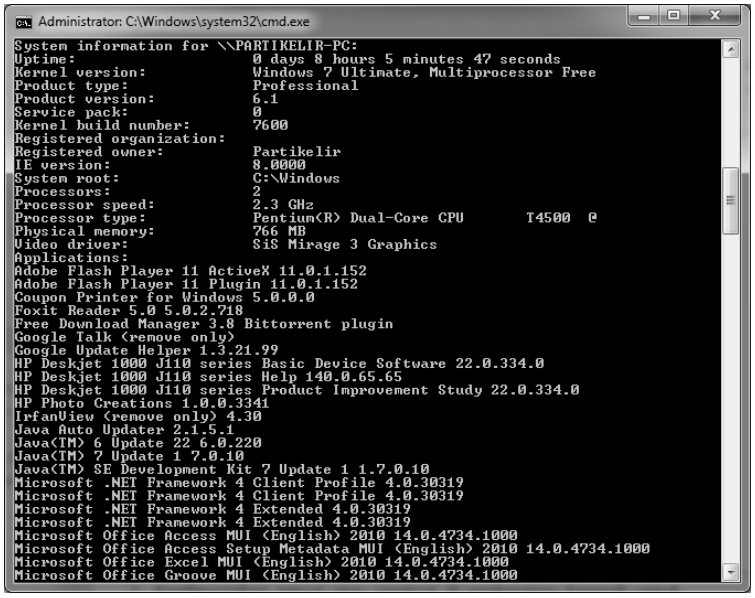
  Mencetak dalam format CSV.

- -t

  Delimiter standar untuk opsi –c adalah koma, tapi bisa ditimpa dengan karakter yang ditentukan.

- filter

  Memfilter Psinfo sehingga hanya menampilkan data dari field yang sesuai dengan filter. Misalnya "psinfo service" hanya menampilkan field service pack.



Gambar 1.15 Contoh penggunaan Psinfo

1.3.9 Mendeteksi Rootkit dengan RootkitRevealer

RootkitRevealer merupakan tool untuk mendeteksi rootkit di komputer. Software ini bisa dijalankan di Windows XP dan Windows Server. Software ini akan menghasilkan output berupa daftar registry dan API sistem file yang mengindikasikan adanya rootkit dalam user-mode atau kernel-mode.

RootkitRevealer bisa mendeteksi berbagai rootkit yang membandel, termasuk di antaranya adalah AFX, Vanquish, dan HackerDefender.

Software ini berbasis GUI dan tidak lagi mendukung versi command line. Sebab para pembuat malware mulai memindai RootkitRevealer menggunakan nama executable-nya. Sehingga software ini di-update untuk mengeksekusi scan dari salinannya yang memiliki nama yang acak, yang berjalan sebagai Windows service.

Tipe pengeksekusian ini tidak bisa diterapkan untuk antarmuka command line. Sehingga terpaksa diubah ke mode GUI.

Apa Itu Rootkit?

Rootkit adalah istilah yang menjelaskan mekanisme dan teknik yang sering dipakai oleh malware, termasuk virus, spyware, dan trojan untuk menyembunyikan kehadirannya dari spyware blocker, antivirus, dan utilitas System management.

Ada beberapa klasifikasi rootkit, tergantung pada apakah malware bisa selamat dari reboot, dan dieksekusi di user mode atau kernel mode.

- Rootkit Persistent

  Rootkit Persistent diasosiasikan dengan malware yang aktif tiap kali sistem booting. Malware biasanya harus menyimpan kode di mode persistent, karena kode ini harus dieksekusi secara otomatis tiap kali sistem dijalankan. Penyimpanannya biasanya di registry atau di sistem file, dan mengonfigurasi metode di mana kode dieksekusi tanpa intervensi user.

- Rootkit Memory-based

  Memory-based rootkit merupakan malware yang tidak punya kode yang persistent sehingga tidak bisa me-reboot.

- Rootkit User-mode

  Ada beberapa metode yang biasa dipakai oleh rootkit untuk meloloskan diri dari pendeteksian. Misalnya Rootkit usermode bisa mencegat semua panggilan ke API Windows FindFirstFile/ FindNextFile, di mana API ini biasanya digunakan oleh utilitas file system exploration, termasuk Explorer dan command prompt.

  Bisa juga untuk enumerasi konten dari direktori sistem file. Ketika aplikasi melakukan listing direktori yang akan mengembalikan hasil yang berisi semua file yang berkaitan dengan rootkit, rootkit akan mencegatnya dan menghapus entri.

  API native dari Windows adalah antarmuka antara client user-mode dan layanan kernel-mode, dan rootkit user-mode bisa mencegat sistem file, registry, dan fungsi enumerasi proses dari API native. Ini bisa dipakai untuk mencegah pendeteksian scanner yang memakai metode pembandingan hasil dari enumerasi Windows API yang dihasilkan oleh enumerasi API.

- Rootkit Kernel-mode

  Rootkit kernel-mode merupakan tipe rootkit yang lebih powerful. Rootkit ini tidak hanya bisa mencegat API native dalam mode kernel, tapi juga bisa digunakan untuk memanipulasi struktur data di mode kernel.

  Teknik yang umum dipakai untuk menyembunyikan proses malware adalah dengan menghapus process dari daftar active process di kernel. Ini karena API process management bergantung pada data content dari list.

Cara Memakai Rootkit Revealer

RootkitRevealer memiliki dua antarmuka GUI dan command line. Untuk memakai rootkitRevealer, usahakan semua aplikasi sedang idle atau tidak dijalankan agar tidak mengganggu proses pemindaian dari RootkitRevealer.

Untuk pemindaian manual, Anda tinggal klik tombol **Scan**. Maka RootkitRevealer akan memindai system dan menampilkan status di status area pada bagian bawah jendela. Beberapa opsi yang bisa Anda gunakan adalah:

- Hide NTFS Metadata Files: opsi ini On secara default, dan rootkitRevealer akan tidak menampilkan file metadata NTFS yang disembunyikan dari Windows API.
- Scan Registry: opsi ini juga On secara default. Menghilangkan pilihan ini akan membuat RootkitRevealer tidak memindai Registry.

Anda juga bisa menjalankan pemindaian otomatis. Sintaks untuk menjalankan program ini adalah:

```
rootkitrevealer [-a [-c] [-m] [-r] outputfile]
```

Penjelasan dari beberapa parameter adalah:

- -a

  Otomatis memindai, kemudian menutup program ketika sudah selesai.

- -c

  Memformat output sebagai CSV.

- -m

  Menunjukkan file metadata NTFS.

- -r

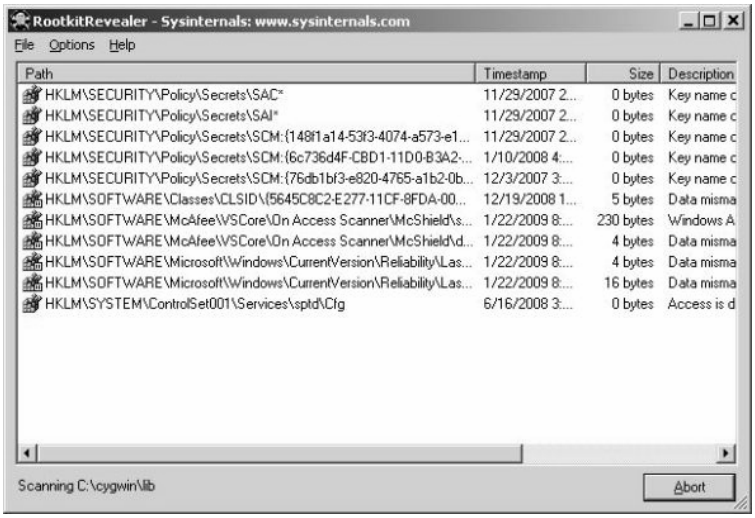
  Tidak memindai registry.

Lokasi output file harus di volume lokal dari hard disk Anda.

Jika Anda menentukan opsi –c, maka tidak ada laporan progress dan perbedaannya akan dicetak di format CSV agar mudah diimpor ke database. Anda bisa memindai sistem remote dengan menjalankan program ini berbarengan dengan PsExec menggunakan perintah seperti berikut:

```
psexec \\remote -c rootkitrevealer.exe -a
c:\windows\rootkit.log
```

RootkitRevealer akan mendeteksi rootkit-rootkit serta data di registry yang mencurigakan.



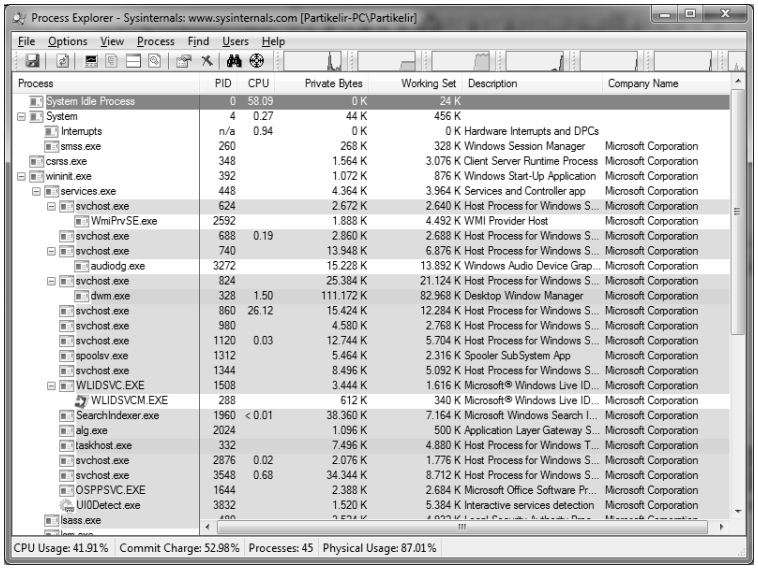
Gambar 1.16 Hasil pemindaian rootkit

1.3.10 Melacak Proses dengan Process Explorer

Process Explorer menunjukkan informasi mengenai apa yang meng-handel proses dan DLL yang dibuka atau di-load.

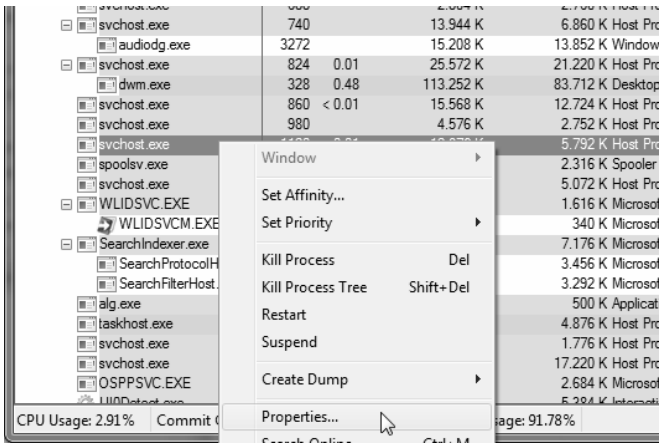
Process Explorer terdiri atas dua jendela. Bagian atas menampilkan active processes, termasuk nama dari akun yang memiliki proses. Sementara informasi ditampilkan di bagian bawah, di mode yang ada di process explorer.

Kegunaan Process Explorer adalah untuk melakukan pelacakan pada masalah DLL dan untuk mengetahui bagaimana cara kerja Windows.



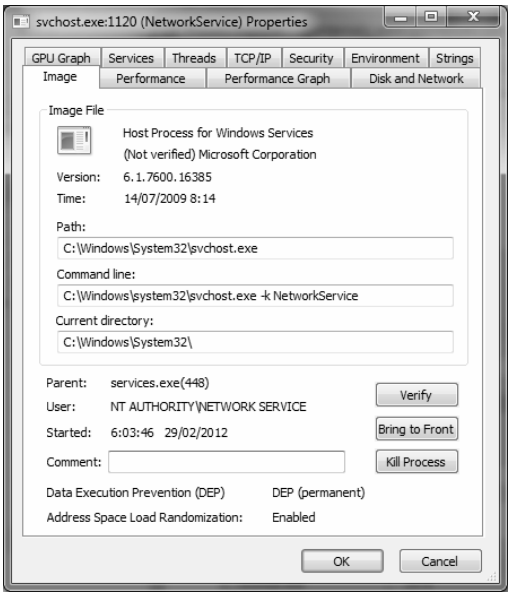
Gambar 1.17 Pemindaian di Process Explorer

Anda juga bisa melihat detail dari tiap proses, termasuk path lengkap dari file yang menjalankan proses itu. Caranya dengan klik kanan pada proses kemudian klik **Properties**.



Gambar 1.18 Menu Properties untuk melihat detail proses

Maka terlihat tampilan seperti berikut ini.



Gambar 1.19 Tampilan detail dari proses di Process Explorer

1.3.11 Memantau Koneksi TCP dengan TCPView

TCPView adalah program Windows yang akan menampilkan listing detail dari semua endpoint TCP dan UDP di komputer Anda. Termasuk alamat lokal dan remote, juga kondisi koneksi TCP.

Di Windows Server 2008, Vista, dan XP, TCPView juga melaporkan nama process yang memiliki endpoint tersebut. TCPView memiliki informasi yang lebih informatif dan nyaman. TCPView memiliki versi command line yang bernama Tcpvcon.

Ketika Anda menjalankan TCPView, program ini akan mengenumerasi semua endpoint TCP dan UDP, mengambil semua IP address ke versi nama domainnya.

Anda bisa menggunakan tombol toolbar atau item menu untuk menampilkan nama yang ditemukan. Secara default, TCPView ini akan di-update tiap detik. Tapi Anda bisa mengatur refresh rate dengan klik pada **Options** > **Refresh Rate**.

Anda bisa meng-close koneksi TCP/IP dengan memilih menu **File > Close Connections** atau dengan klik kanan dan memilih **Close Connections** dari context menu. Anda bisa menyimpan jendela output dari TCPView dengan menu **Save**.

Untuk menggunakan, contoh sintaksnya adalah:

```
tcpvcon [-a] [-c] [-n] [nama_proses atau PID]
```

Beberapa penjelasan parameter di atas adalah:

- -a

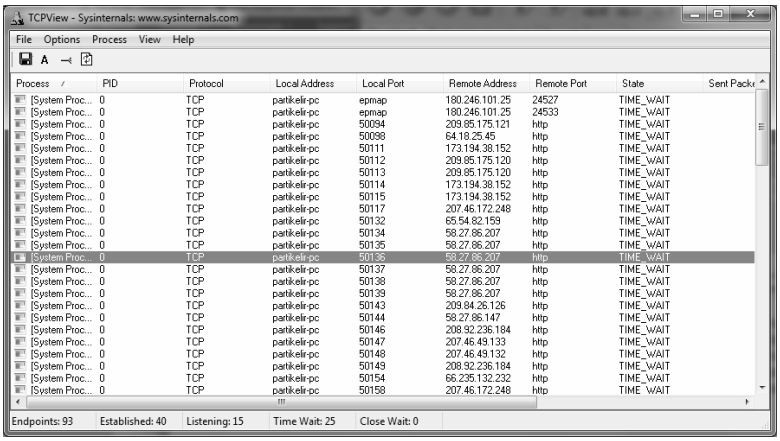
  Menampilkan semua endpoint (default-nya menampilkan koneksi TCP yang sudah ada).

- -c

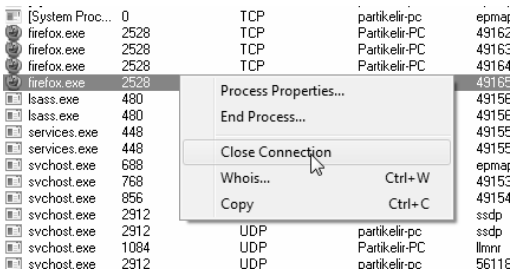
  Mencetak output sebagai CSV.

- -n

  Jangan resolve address.



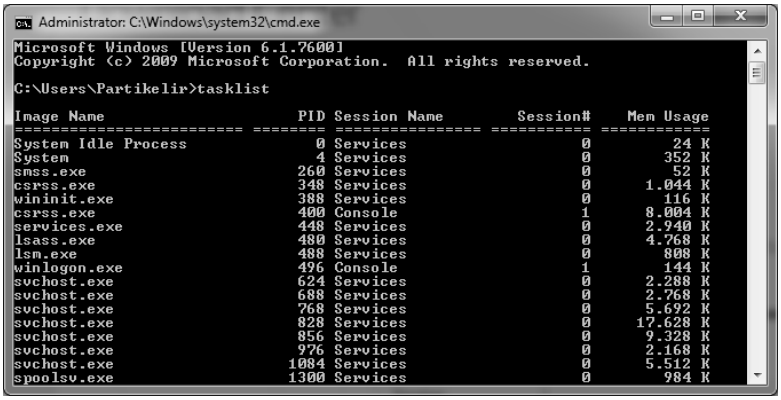
Gambar 1.20 TCP View



Gambar 1.21 Tampilan untuk Close Connection

1.3.12 Melihat Task Berjalan dengan TaskList

Ini merupakan perintah command line untuk melihat task list di command prompt. Anda bisa menggunakan ini untuk mencari tahu task apa saja yang berjalan di komputer Anda.



Gambar 1.22 Task list di command line untuk menjalankan task list

TaskList akan menampilkan daftar aplikasi dan layanan-layanan bersama dengan Process ID (PID) untuk semua tugas yang sedang dijalankan pada komputer lokal atau komputer remote.

Sintaksnya adalah:

```
tasklist[.exe] [/s computer] [/u domain\user [/p password]]
[/fo {TABLE|LIST|CSV}] [/nh] [/fi FilterName [/fi FilterName2
[ ... ]]] [/m [ModuleName] | /svc | /v]
```

Keterangan dari parameter yang digunakan adalah:

- /s computer

  Menentukan nama atau IP Address dari komputer remote. Jangan gunakan backslash. Nilai default-nya adalah komputer lokal.

- /u domain \user

  Menjalankan command dengan account permission dari user tertentu. Nilai default adalah permission dari user yang sedang login.

- /p password

  Menentukan password dari user account yang ditentukan di parameter /u.

- /fo { TABLE | LIST | CSV }

  Menentukan format yang digunakan untuk output. Nilai valid adalah TABLE, LIST, dan CSV. Format default untuk output adalah TABLE.

- /nh

  Menyembunyikan header kolom di output. Valid ketika parameter /fo diset ke TABLE atau CSV.

- /fi FilterName

  Menentukan tipe proses untuk dimasukkan atau dikeluarkan dari query.

- /m [ModuleName]

  Menentukan untuk menampilkan informasi modul tiap proses. Ketika sebuah modul ditentukan, semua proses yang memakai modul tersebut akan ditampilkan. Ketika modul tidak diten-tukan, semua proses untuk semua modul disampaikan. Ini tidak bisa dipakai dengan parameter /svc atau /v.

- /svc

  Menampilkan semua informasi service untuk proses tanpa potongan. Ini valid ketika parameter /fo diset ke TABLE. Tidak bisa digunakan dengan parameter /m atau /v.

- /v

  Menentukan task information verbose untuk ditampilkan di output. Tidak bisa digunakan dengan parameter /svc atau /m.

- /?

  Menampilkan bantuan di command prompt.

1.3.13 Mematikan Komputer dengan PsShutdown

PsShutdown adalah tool command line yang merupakan utility untuk shutdown, yang bisa mematikan komputer lokal atau remote, setelah Anda mengumpulkan data.

PsShutdown juga bisa me-logoff konsol atau me-lock konsol. Anda bisa menggunakan PsShutdown untuk memulai shutdown dari komputer remote dan lokal. Anda juga bisa membatalkan sebuah shutdown yang telah dijadwalkan. Berikut ini contoh sintaks untuk PsShutDown:

```
psshutdown [[\\computer[,computer[,..] | @file [-u user [-p
psswd]]] -s|-r|-h|-d|-k|-a|-l|-o [-f] [-c] [-t nn|h:m] [-n s]
[-v nn] [-e [u|p]:xx:yy] [-m "message"]
```

Berikut ini beberapa parameter argumen yang bisa dipakai untuk psShutDown:

- - computer

  Menerapkan command pada komputer remote atau komputer yang ditentukan. Jika Anda menghilangkan nama komputer, command akan berjalan di sistem lokal. Jika Anda mengisikan tanda bintang (*), maka command berjalan di semua komputer pada domain yang ada.

- @file

  Menjalankan command pada tiap komputer yang ada di file teks tertentu.

- -u

  Menentukan username opsional untuk login ke komputer remote.

- -p

  Menentukan password opsional untuk username. Jika Anda menghilangkan ini, maka Anda akan dimintai password secara manual.

- -a

  Membatalkan proses shutdown (hanya bisa digunakan ketika hitungan mundur sedang dilakukan).

- -c

  Memungkinkan shutdown dibatalkan oleh user interaktif.

- -d

  Men-suspend komputer.

- -e

  Kode alasan untuk shutdown. Anda bisa mengisikan 'u' untuk alasan user, dan 'p' untuk kode alasan terencana. Kode xx merupakan kode alasan paling lazim dipakai (ini harus di bawah 256). Kode yy merupakan kode alasan minor (harus kurang dari 65536).

- -f

  Memaksakan semua aplikasi yang sedang berjalan untuk keluar selama shutdown.

- -h

  Menghibernasi komputer.

- -k

  Mematikan komputer (reboot jika poweroff tidak didukung).

- -l

  Me-lock komputer.

- -m

  Anda bisa menentukan pesan untuk ditampilkan ke user yang login ketika mengaktifkan hitung mundur untuk shutdown.

- -n

  Menentukan timeout dalam satuan detik ketika hendak konek ke komputer remote.

- -o

  Logoff konsol user.

- -r

  Reboot setelah shutdown.

- -s

  Shutdown tanpa power off.

- -t

  Menentukan hitung mundur dalam detik (defaultnya adalah 20 detik) atau waktu shutdown (dalam waktu 24 jam).

- -v

  Menampilkan pesan untuk waktu tertentu sebelum shutdown.

1.3.14 Menampilkan Daftar File yang Diakses secara Remote dengan PsFile

Perintah "net file" memberitahukan Anda daftar file yang sudah dibuka di komputer lain. Tapi nama file-nya dipotong, dan Anda juga tidak bisa melihat informasi untuk sistem remote.

PsFile merupakan utility command line yang menampilkan daftar file di sistem yang dibuka secara remote. Ini juga memungkinkan Anda menutup file yang terbuka, baik dengan namanya atau identifier file-nya.

Anda bisa menggunakan perintah berikut:

```
Usage: psfile [\\RemoteComputer [-u Username [-p Password]]]
[[Id | path] [-c]]
```

Penjelasan dari beberapa parameter argumen di atas adalah:

- -u

  Menentukan username untuk login ke komputer remote (opsional).

- -p

  Menentukan password untuk username. Jika ini tidak dimasukkan, Anda akan dimintai secara manual.

- Id

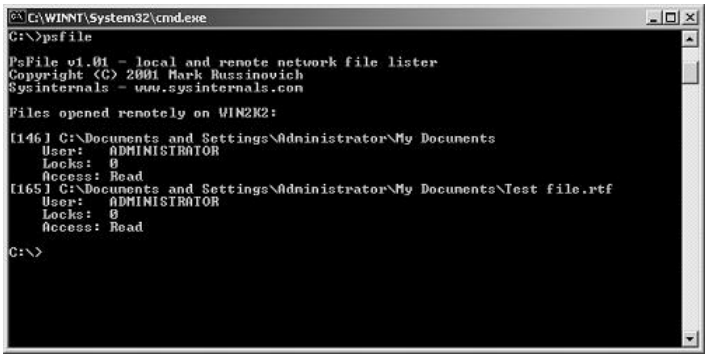
  Identifier dari file yang ingin ditampilkan informasinya, atau yang ingin di-close.

- Path

  Path lengkap atau sebagian yang berkaitan dengan informasi untuk di-display atau dimatikan.

- -c

  Menutup file yang ditentukan oleh ID atau path.



Gambar 1.23 Mengetahui file yang diakses secara remote dari PsFile

1.3.15 Me-remote Sistem Lain dengan PsExec

Utility seperti telnet dan program remote control seperti PC Anywhere dari Symantec memungkinkan Anda mengeksekusi program di sistem remote. Tapi ini repot konfigurasinya, karena Anda perlu menyeting software klien di sistem remote yang akan dijalankan.

PsExec merupakan pengganti telnet yang memungkinkan Anda meng-eksekusi proses di sistem lain dengan tingkat interaktivitas yang cukup lumayan khusus untuk aplikasi konsol.

Anda tidak harus menginstal software client, karena PSExec bisa digunakan untuk menjalankan command prompt di sistem remote dan mengaktifkan tool seperti IpConfig secara langsung.

Catatan: Beberapa antivirus kadang melaporkan tool ini dicurigai sebagai virus 'remote admin'. Tapi sebenarnya tidak ada virus di tool ini.

Sintaks untuk psexec ini adalah:

```
psexec [\\computer[,computer2[,...] | @file][-u user [-p
psswd]][-n s][-l][-s|-e][-x][-i [session]][-c [-f|-v]][-w
directory][-d][-<priority>][-a n,n,... ] cmd [arguments]
```

Penjelasan dari beberapa parameter argumen yang digunakan adalah:

- computer

  Mengarahkan PsExec untuk menjalankan aplikasi di satu komputer atau lebih yang ditentukan. Jika Anda menghilangkan nama komputer, PsExec akan dijalankan di komputer lokal. Jika Anda mengisikan "*", PsExec akan menjalankan aplikasi di semua komputer pada domain yang ada sekarang.

- @file

  Mengarahkan PsExec untuk menjalankan command pada tiap komputer yang ditulis di file teks tertentu.

- -a

  Memisahkan prosesor pada aplikasi yang menjalankan aplikasi, di mana nomor 1 menunjukkan CPU dengan prioritas terendah, sementara yang berikutnya tertinggi. Ini dipisahkan dengan koma. Contohnya "-a 2,4" untuk menjalankan di prosesor kedua dulu, baru keempat.

- -c

  Menyalin program tertentu ke sistem remote untuk dieksekusi. Jika Anda menghilangkan opsi ini, maka aplikasi harus ada di path tertentu pada sistem remote.

- -d

  Perintah agar aplikasi tidak menunggu untuk dimatikan. Anda hanya boleh menggunakan ini untuk aplikasi yang tidak interaktif.

- -e

  Tidak me-load profil akun tertentu.

- -f

  Menyalin program tertentu ke sistem remote, walaupun file sudah ada di sistem remote.

- -i

  Menjalankan program sehingga bisa berinteraksi dengan desktop pada sesi tertentu di sistem remote. Jika tidak ada session yang ditentukan, maka proses dijalankan di session konsol.

- -l

  Menjalankan proses sebagai user terbatas. Di Windows 7, ini akan menjalankan proses dengan integritas rendah.

- -n

  Menentukan timeout dalam satuan detik ketika melakukan koneksi ke komputer remote.

- -p

  Menentukan password untuk username (opsional). Jika tidak diberikan, Anda perlu memasukkannya secara interaktif.

- -s

  Menjalankan proses remote di akun sistem.

- -u

  Menentukan username untuk login ke komputer remote (opsional).

- -v

  Menyalin file hanya jika versi yang ada di komputer remote lebih baru.

- -w

  Mengeset direktori kerja dari proses relatif ke komputer remote.

- -x

  Menampilkan antarmuka dari desktop Winlogon (hanya di komputer lokal saja).

- -priority

  Menentukan prioritas, apakah -low, -belownormal, -abovenormal, -high, atau -realtime untuk menjalankan proses pada berbagai prioritas yang berbeda. Gunakan background untuk menjalankan pada memori rendah dan prioritas I/O di Windows 7.

- program

  Nama dari program yang akan dieksekusi.

- arguments

  Argumen yang akan diberikan di sistem target.

Anda bisa menutup aplikasi yang punya spasi di namanya dengan menggunakan tanda petik dua. Misalnya: "psexec \\marklap "c:\nama panjang\app.exe". Input ini hanya akan dikirimkan ke sistem remote kalau Anda menekan tombol Enter. Dan mengetikkan CTRL + C untuk mematikan proses remote.

Jika Anda tidak menggunakan username, maka proses remote akan dijalankan di akun yang sama di mana Anda mengeksekusi PsExec. Contoh penggunaannya ketika hendak mengeksekusi di komputer bernama \\lab01 adalah:

```
psexec \\lab01 cmd
```

Perintah ini akan mengekskusi IpConfig di sistem remote dengan /all switch, dan menampilkan hasilnya secara lokal.

```
psexec \\lab01 ipconfig /all
```

Perintah ini akan menyalin program test.exe ke komputer remote dan mengeksekusinya secara interaktif.

```
psexec \\lab01 -c test.exe
```

Ini akan menentukan path penuh ke program yang sudah terinstal di sistem remote tapi tidak ada di path sistem.

```
psexec \\lab01 c:\bin\test.exe
```

Sementara berikut ini akan menjalankan regedit secara interaktif di akun sistem untuk melihat konten dari key SAM dan Security.

```
psexec -i -d -s c:\windows\regedit.exe
```

Sementara contoh berikut untuk menjalankan Internet Explorer dengan user privilege:

```
psexec -l -d "c:\program files\internet explorer\iexplore.exe"
```

1.3.16 Mengontrol Service dengan PsService

PsService merupakan service viewer dan controller untuk Windows. Software ini memungkinkan Anda untuk melakukan start, stop, pause, resume, dan restart service secara live dan command line.

Tidak seperti utility SC, PsService memungkinkan Anda untuk logon ke sistem remote menggunakan berbagai akun. PsService memiliki kemampuan pencarian service unik yang memungkinkan identifikasi instance yang aktif dari service di jaringan Anda.

Anda bisa memakai fitur search pada kasus seperti ketika Anda ingin mengetahui sistem yang berjalan di DHCP server.

PsService akan menampilkan service di sistem lokal. Sintaks yang bisa dipakai untuk menggunakan psservice adalah:

```
psservice [\\computer [-u username] [-p password]] <command>
<options>
```

Beberapa parameter untuk sintaks ini adalah:

- query

  Menampilkan status dari service.

- config

  Menampilkan konfigurasi dari service.

- setconfig

  Mengeset tipe start, disabled, auto, demand dari service.

- start

  Memulai service.

- stop

  Menghentikan service.

- restart

  Menghentikan dan me-restart service.

- pause

  Menghentikan service untuk sementara.

- cont

  Melanjutkan service yang dihentikan sementara.

- depend

  Menampilkan daftar service yang punya ketergantungan dengan service lainnya.

- security

  Membuang deskriptor sekuriti dari service.

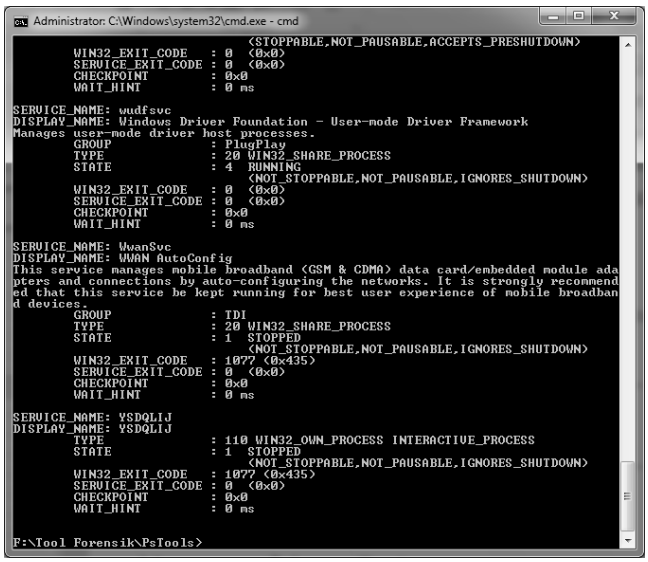
- find

  Mencari service di jaringan tertentu.

- \\computer

  Login ke sistem remote. Anda akan diminta username dan password atau bisa juga mengisikannya langsung di parameter.

PsService bisa melakukan ini karena menggunakan API dari Service Control Manager.



Gambar 1.24 PsService menampilkan daftar service

1.3.17 Menerjemahkan SID dengan PsGetSid

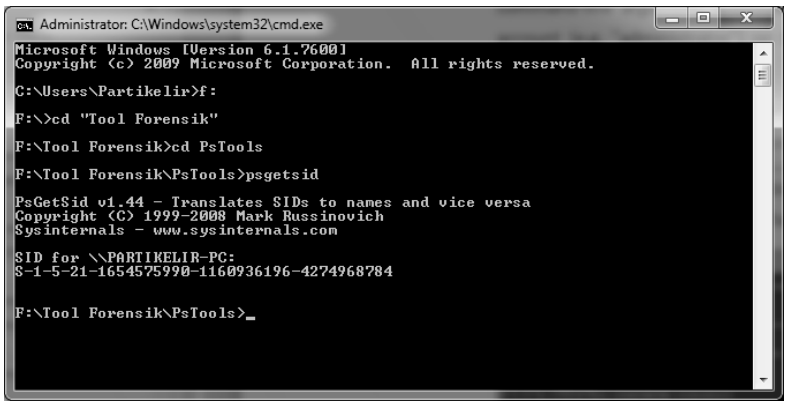
PsGetsid memungkinkan Anda menerjemahkan SID ke nama display-nya, dan kebalikannya. Ini bisa diterapkan untuk akun built-in, akun domain, dan akun lokal.

Sintaks untuk menggunakan PsGetSID adalah:

```
psgetsid [\\computer[,computer[,...] | @file] [-u username [-p
password]]] [account|SID]
```

Jika Anda ingin tahu SID dari sebuah komputer, Anda tinggal mengisikan nama komputer di parameter argumen. Kalau mau tahu SID dari user, Anda bisa mengisikan nama akun (misalnya “administrator”) di command line.

Anda bisa menentukan username di akun yang Anda jalankan yang tidak memiliki hak administratif. Jika Anda tidak memasukkan password, maka PsGetSID akan meminta Anda secara langsung.



Gambar 1.25 PsGetSid