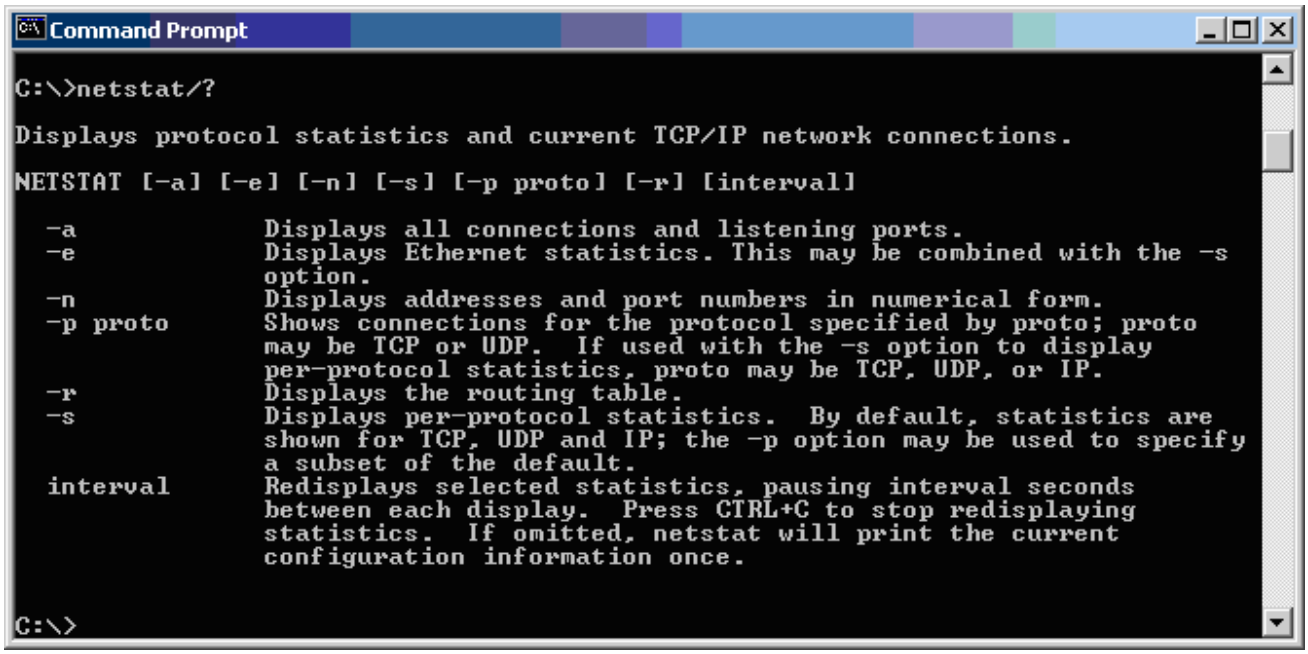
การใช้โปรแกรม NETSTAT

Netstat เป็นคำสั่งที่ใช้ตรวจสอบ Network เกี่ยวกับการเชื่อมต่อ Port ในเครื่องเรากับเครื่องอื่นใน Network



จากการใช้คำสั่งจาก DOS Prompt ในรูปข้างบน เป็นการเรียกดูวิธีการใช้ของโปรแกรม netstat โดยการใส่เครื่องหมาย /? ต่อท้ายคำสั่งนั้น (สามารถใช้ได้กับ โปรแกรมอย่างอื่นในดอสได้ด้วย) เพื่อขอดูการใช้งาน โดยจะอธิบายที่ละบรรทัดอย่างคร่าวๆ

และการใช้คำสั่งนี้ ไม่ว่าจะเป็น Opiton หรือใดๆก็ตาม จะไม่เป็นอันตรายต่อเครื่อง รวมทั้งระบบ Network ซึ่งในการใช้สามารถใช้ได้ในขณะที่ต่อ Internet หรือไม่ก็ตาม

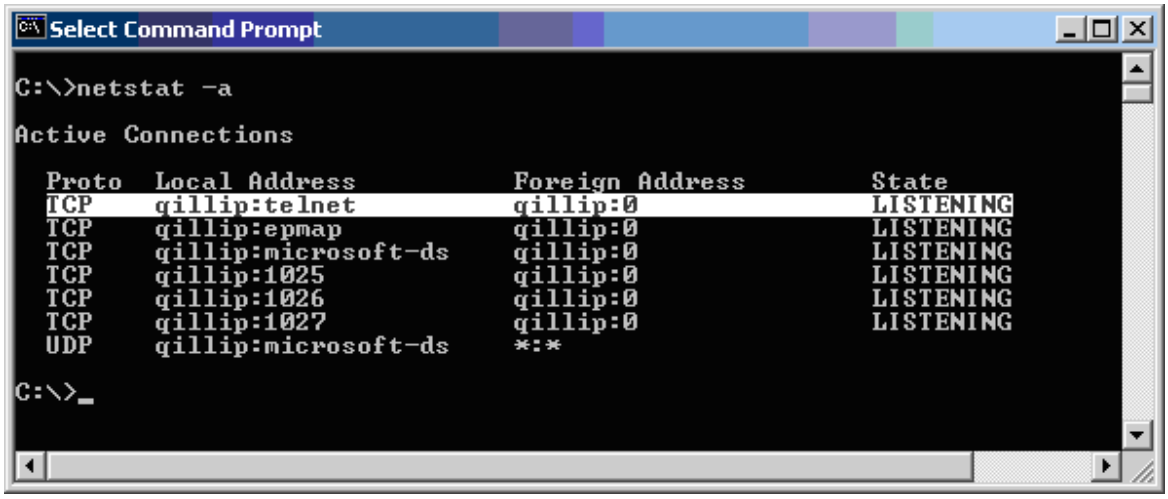
-a Displays all connections and listening ports.
Opiton นี้จะเป็นการดูการเชื่อมต่อ Port ทั้งหมดที่(เครื่องนั้นๆ=เครื่องคุณ)ที่ใช้คำสั่งนี้ ได้เปิดรอการเข้ามาติดต่อ แต่ผลที่แสดงจะเป็นรายชื่อ Service ที่ติดต่อกับเครื่อง(เครื่องนั้นๆ=เครื่องคุณ) เช่นชื่อเว็บไซต์ หรือชื่อเครื่อง ไม่แสดงเป็นตัวเลข IP

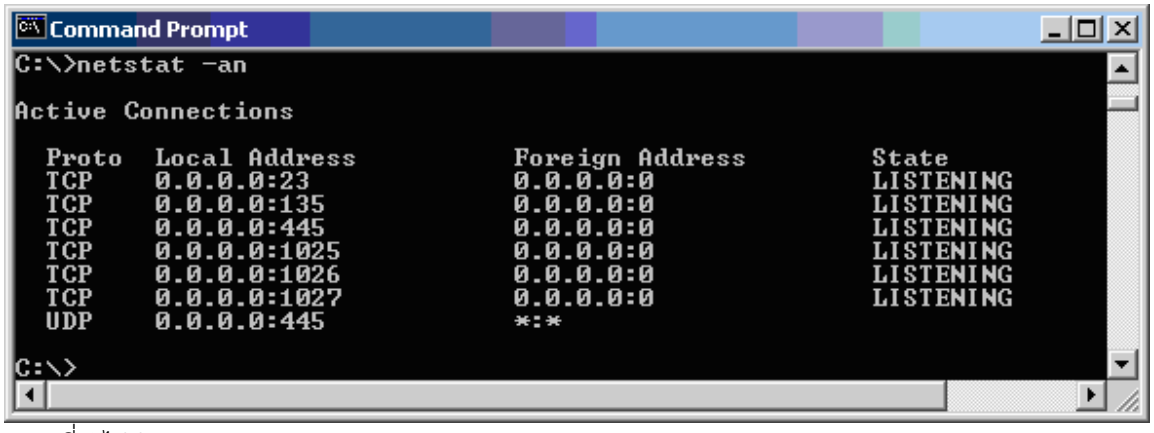
-e Displays Ethernet statistics. This may be combined with the -s
option.

Opiton นี้จะเป็นการดูเหมือนกับสถิติต่าง ในการรับ/ส่งข้อมูลต่าง ต้องใช้ร่วมกับ Opiton -s เป็นการดูสถานะการรับส่งข้อมูลต่าง ซึ่งลองใช้ดูได้

-n Displays addresses and port numbers in numerical form.
Opiton นี้จะเหมือนกับ -a แต่การแสดงผลจะเป็น เลข IP กับ Port แทนชื่อเครื่อง หรือชื่อเว็บไซด์ต่างๆ ที่ได้มีการติดต่อ หรือเชื่อมการติดต่อ

การใช้งาน netstat (แบบดอส)
สังเกตว่า 2 ภาพด้านล่างเป็นการใช้ 2 option การแสดงผลก็ต่างกันนิดหน่อย แต่ความหมายแต่ละบรรทัด มีค่าเท่ากันเพียงแต่การแสดงแตกต่างเป็น ชื่อ กับ ตัวเลข (เลข IP/Prot) นั่นเอง





(ขณะที่ยังไม่ต่อ Internet)

สังเกตเฉพาะบรรทัดที่ได้ทำเป็น แถบสีขาวก่อน (รูปด้านบน 2 รูป)

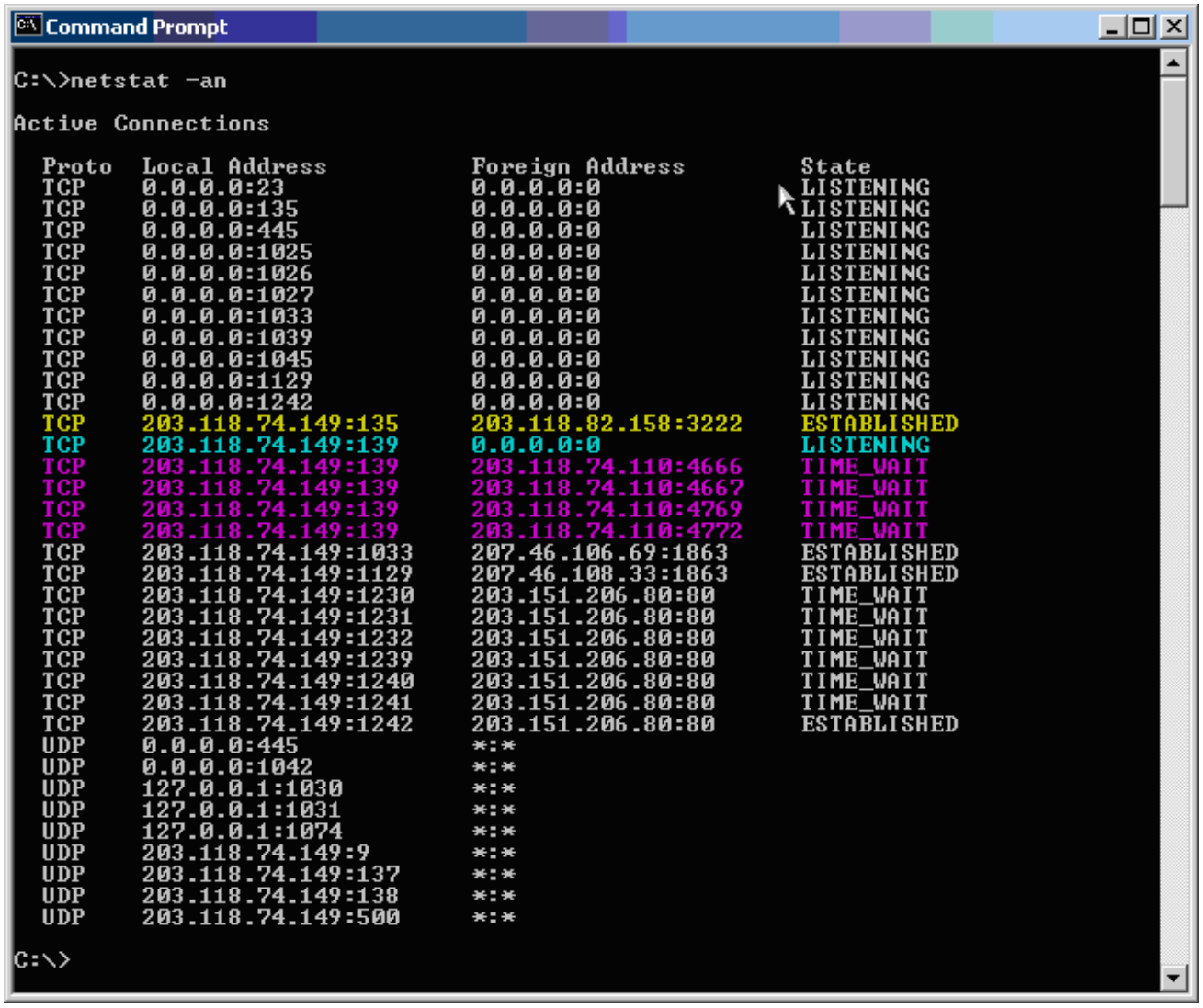
1. Proto ->TCP คือโปรโตคอลที่เครื่องกำลังเชื่อมต่ออยู่

2. Local Address -> qillip:telnet [ชื่อเครื่อง qillip] : [telnet Service (port ที่เครื่องได้เปิด)] ซึ่งตอนนี้เป็นหรือบริการที่เปิดและเราจะรู้ได้ตรงนี้เอง เช่นพวกโทรจัน Trojan หรือโปรแกรมบางโปรแกรมมักจะเปิด Service หรือบริการที่เปิดรอ เพื่อจะเข้ามาควบคุมเครื่อง หรือมีการแชร์เครื่อง เพื่อใช้ในการถ่ายโอนข้อมูลระหว่างเครื่อง ในระบบ Network

3. Foreign Address -> qillip:0 ชื่อเครื่อง [qillip] : [เครื่องที่เชื่อมต่อกับเครื่องที่คุณได้ใช้อยู่] ที่เป็นเลข 0 เพราะว่ายังไม่ได้ต่อเน็ต

4. State -> LISTENING สถานะการติดต่อซึ่งจะมีอยู่หลายแบบคือ ตรงนี้ขอข้ามไปก่อนครับว่าหมายถึงอะไร และต่อจากนี้ เพื่อให้เข้าใจง่ายขึ้น จะขอยกตัวอย่าง ข้ามขั้นตอน เพราะปรกติแล้ว การใช้งานทั่วไป มักจะใช้คำสั่ง C:\>netstat -an หรือ C:\>netstat -a เวลาใช้ พิมพ์แค่ netstat -a หรือ netstat -an ที่ Dos Prompt เพราะว่า จะทำให้มีการดูเป็นรูปแบบที่ง่ายขึ้น ส่วน option อื่นลองไปใช้เองดู ซึ่งใช้เดี่ยวๆ หรือคู่กันไปก็ได้ ที่ได้แนะนำมาแบบนี้ คำสั่งทั้ง 2 ตัวที่ได้ยกขึ้นมานี้ได้ครอบคลุมการดูเกือบทั้งหมดแล้ว เพียงแต่ต้องไปศึกษาว่า port แต่ละหมายเลขเป็นบริการของอะไร เป็นโทรจันหรือไม่ อาจเป็นโปรแกรม remote ก็ได้ ซึ่งโปรแกรม remote จะสามารถหลบการสแกนจากโปรแกรม Anti Virus / Trojan Scan

จากตัวอย่างที่ได้ทำเป็นแถบสีขาวให้ดูจาก 2 รูปด้านบนที่บริการที่ได้เปิด Local Address=qillip:telnet ตรง telnetเราต้องรู้ว่า telnet คือ port 23 หรืออาจพิมพ์คำสั่ง netstat -an เพื่อตรวจดูหมายเลข port ซึ่งจะอยู่บรรทัดเดียวกัน ดัง 2 รูปข้างต้น (ถ้าใช้ในเวลาเดียวกัน 2 Option ทั้ง -a และ -an และ -nเราลองใช้ดูครับ การแสดงผลจะได้ค่าที่เหมือนกัน แต่แตกต่างที่จะเป็น ชื่อบริการเราได้เปิดหรือ เป็นแบบ ตัวเลข IP)



(ตอนนี้ได้ต่อ Internet แล้ว)

สีเหลือง เป็นสถานะ ESTABLISHED

Local Address คือ IP ที่ได้คือ 203.118.74.149 ได้เปิด port 135 เอาไว้และเข้ามาที่เครื่องทาง port นี้

Foreign Address เป็น IP ของเครื่องที่มา hack เครื่องคือ 203.118.82.158

State เป็นสถานะ ESTABLISHED หมายความว่า เป็นการเชื่อมต่อระหว่างเครื่อง 2 เครื่องได้แล้ว พูดอีกแบบคือ มีเครื่องอื่นได้เข้ามาในเครื่องนี้แล้ว

สีฟ้า เป็นสถานะ LISTENING

Local Address คือ IP ที่ได้คือ 203.118.74.149 ได้เปิด port 139

Foreign Address ยังไม่มีเครื่องใดมาทำการติดต่อ

State เป็นสถานะ LISTENING คือรอการติดต่อ ซึ่งเครื่องอื่นสามารถเข้าได้ทางนี้

ให้สังเกตเครื่องคุณถ้าได้มีตัวนี้ อยู่บรรทัดไหน ให้สังเกตที่บรรทัดเดียวกันเราได้เปิด Port ไหนเอาไว้บ้าง

สีม่วง เป็นสถานะ TIME_WAIT

Local Address คือ IP ที่ได้คือ 203.118.74.149 ได้เปิด port 139

Foreign Address เครื่อง ที่มี IP 203.118.74.110 ได้กำลังแสกนเครื่องนี้อยู่ เพื่อหาช่องโหว่

State เป็นสถานะ TIME_WAIT คือเครื่องอื่นกำลังแสกนเครื่องนี้โดยผ่าน port 139 กำลังแสกน หรืออีกความหมาย คือเครื่องนั้นอาจกำลัง ถอด passwordเราอยู่ก็ได้

TIP - ซึ่งตอนนี้คุณคงอ่านและคงสามารถที่จะเดาได้ว่าแต่ละบรรทัดที่โปรแกรมแสดงหมายความว่าอะไรบ้าง แต่ถ้าใช้ Option ดังรูปข้างบน (ต่อ Internet) ให้พิมพ์คำสั่ง netstat -a เพื่อจะแสดงเป็นชื่อ ซึ่งบางที ในสถานะ ESTABLISHED หมายความว่ามีเครื่องอื่นได้เข้ามาในเครื่องเราแล้ว นั้น อาจเป็นเว็บไซต์ที่คุณกำลัง ดาว์นโหลดอยู่ก็ได้ คำสั่ง netstat -a จะแสดงเป็นชื่อเว็บต่างๆ ซึ่งถ้าใช้คำสั่ง netstat -an จะแสดงเป็น ตัวเลข IP ยากต่อการเดา และการดูจริงๆเราต้องสังเกตที่ portเราด้วย ว่าเป็น port ที่ใช้ทำอะไร

HACK -ถ้าคุณกำลัง chat อยู่ไม่ว่าจะเป็น icq , msn , yahoo ect.. ก็ตามและได้มีการรับ/ส่งไฟล์ระหว่างเครื่องเกิดขึ้น ให้พิมพ์คำสั่ง netstat -an หรือ netstat -a หรือ netstat -n ก็ได้ โปรแกรมนี้จะมีการแสดงเลข IP ต่างๆที่คุณได้ติดต่ออยู่ และคุณรู้ IP เครื่องเป้าหมายแล้ว อิอิ ถ้ามีความรู้ในเรื่องอื่น ก็นำมาใช้ได้เลย

นี่คือการทำงานโดยใช้ ดอส แบบทั่วไป ให้คุณลองดูว่าเครื่องคุณได้เปิด Port อะไรไว้บ้าง ถ้ามีการเปิดที่เยอะมากเราต้องรู้ว่าแต่ละ Port ไหนโปรแกรมอะไรเป็นตัวเปิด โดยทำการค้นหาได้จากโปรแกรมที่คุณใช้ได้ถนัด ซึ่งแล้วแต่คนจะถนัดทางไหน และหัวข้อต่อไป จะอธิบายการใช้โปรแกรมอีกตัว ซึ่งใช้ได้ดีมาก สำหรับการหาโปรแกรมตัวแสบ ที่แอบมาเปิด port และยังสามารถใช้งานได้อีกหลายอย่าง แทนโปรแกรม NETSTAT ได้ดีอีกด้วย แถมยังมีโปรแกรมให้ HACK เครื่องแถมมาด้วย

PORT - WINDOW นั้น เปิด port ไหน เป็นมาตรฐาน ?

98+me จะเปิด port 139,445

2000pro 139,445

2000 Advance Server 53,88,139,445

TROJAN PORT

31,Master Paradise

6669,Vampire 1.0

121,BO jammerkillahV

456,HackersParadise

555,Phase Zero

666,Attack FTP

1001,Silencer

1001,Silencer

1001,WebEx

1010,Doly Trojan 1.30 (Subm.Cronco)

1011,Doly Trojan 1.1+1.2

1015,Doly Trojan 1.5 (Subm.Cronco)

1033,Netspy

1042,Bla1.1

1170,Streaming Audio Trojan

1207,SoftWar

1243,SubSeven

1245,Vodoo

1269,Maverick's Matrix

1492,FTP99CMP

1509,PsyberStreamingServer Nikhil G.

1600,Shiva Burka

1807,SpySender

1981,ShockRave

1999,Backdoor

1999,Transcout 1.1 + 1.2

2001,DerSpaeher 3

2001,TrojanCow

2023,Pass Ripper

2140,The Invasor Nikhil G.

2283,HVL Rat5

2565,Striker

2583,Wincrash2

2801,Phineas Nikhil G.

6670,Deep Throat

6883,DeltaSource (DarkStar)

6912,Shitheep

6939,Indoctrination

7306,NetMonitor

7789,iCkiller

9872,PortalOfDoom

9875,Portal of Doom

9989,iNi-Killer

9989,InIkiller

10607,Coma Danny

11000,SennaSpyTrojans

11223,ProgenicTrojan

12076,Gjamer

12223,Hackด99 KeyLogger

12346,NetBus 1.x (avoiding Netbuster)

12701,Eclipse 2000

16969,Priotrity

20000,Millenium

20034,NetBus Pro

20203,Logged!

20203,Chupacabra

20331,Bla

21544,GirlFriend

21554,GirlFriend

22222,Prosiak 0.47

23456,EvilFtp

27374,Sub-7 2.1

29891,The Unexplained

30029,AOLTrojan1.1

30100,NetSphere

30303,Socket25

3791,Total Eclypse (FTP)

4567,FileNail Danny

4950,IcqTrojan

4950,IcqTrojen

5000,Socket23

5011,OOTLT

5031,NetMetro1.0

5400,BladeRunner

5400,BackConstruction1.2

5521,IllusionMailer

5550,XTCP 2.0 + 2.01

5569,RoboHack

5742,Wincrash

6400,The tHing

30999,Kuang

31787,Hack'a'tack

33911,Trojan Spirit 2001 a

34324,Tiny Telnet Server

34324,BigGluck TN

40412,TheSpy

40423,Master Paradise

50766,Fore

53001,RemoteWindowsShutdown

54320,Back Orifice 2000 (default port)

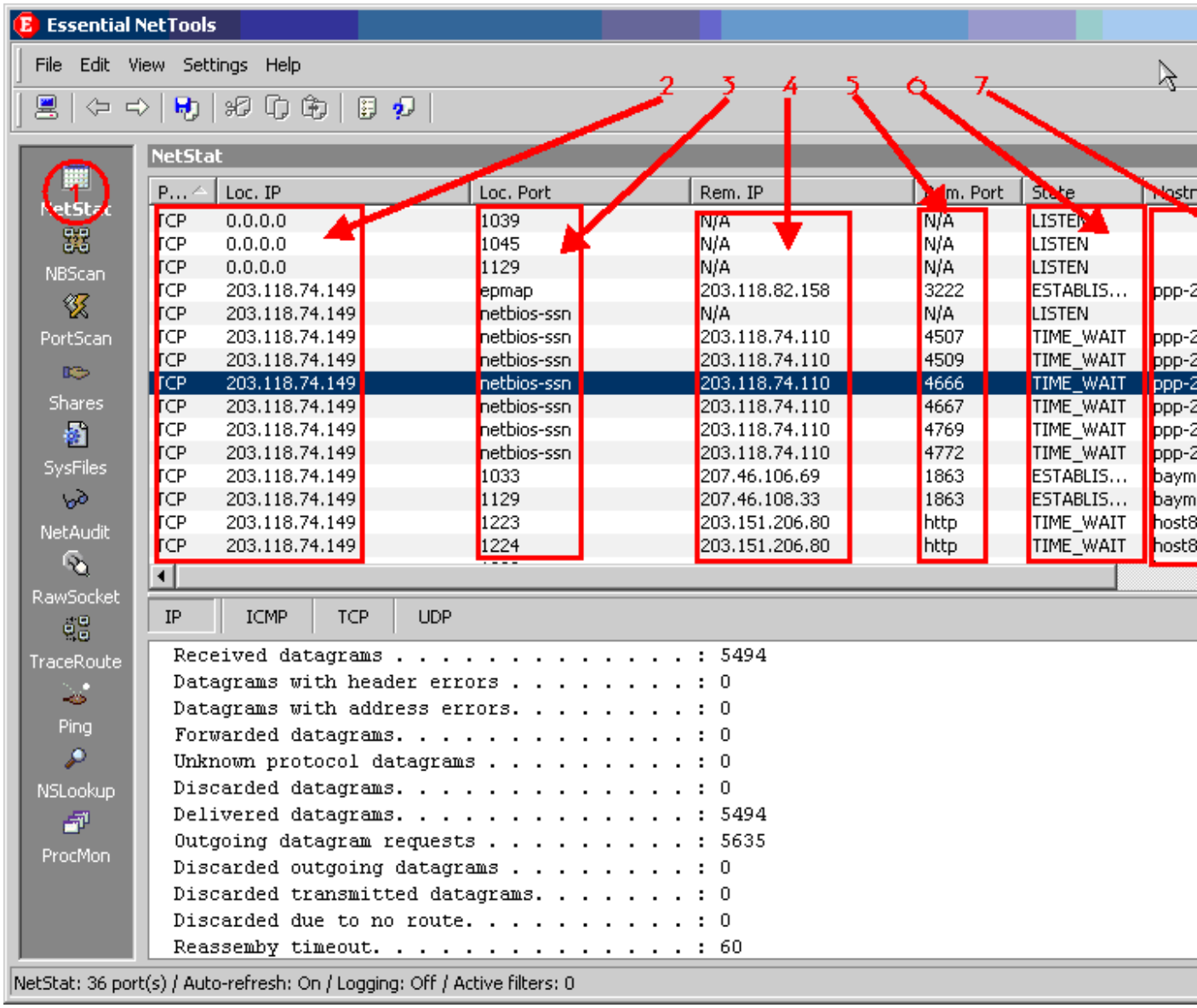
54321,Schoolbus 1.6+2.0

61466,Telecommando

65000,Devil 1.03

การใช้งานโปรแกรม Essential NetTools

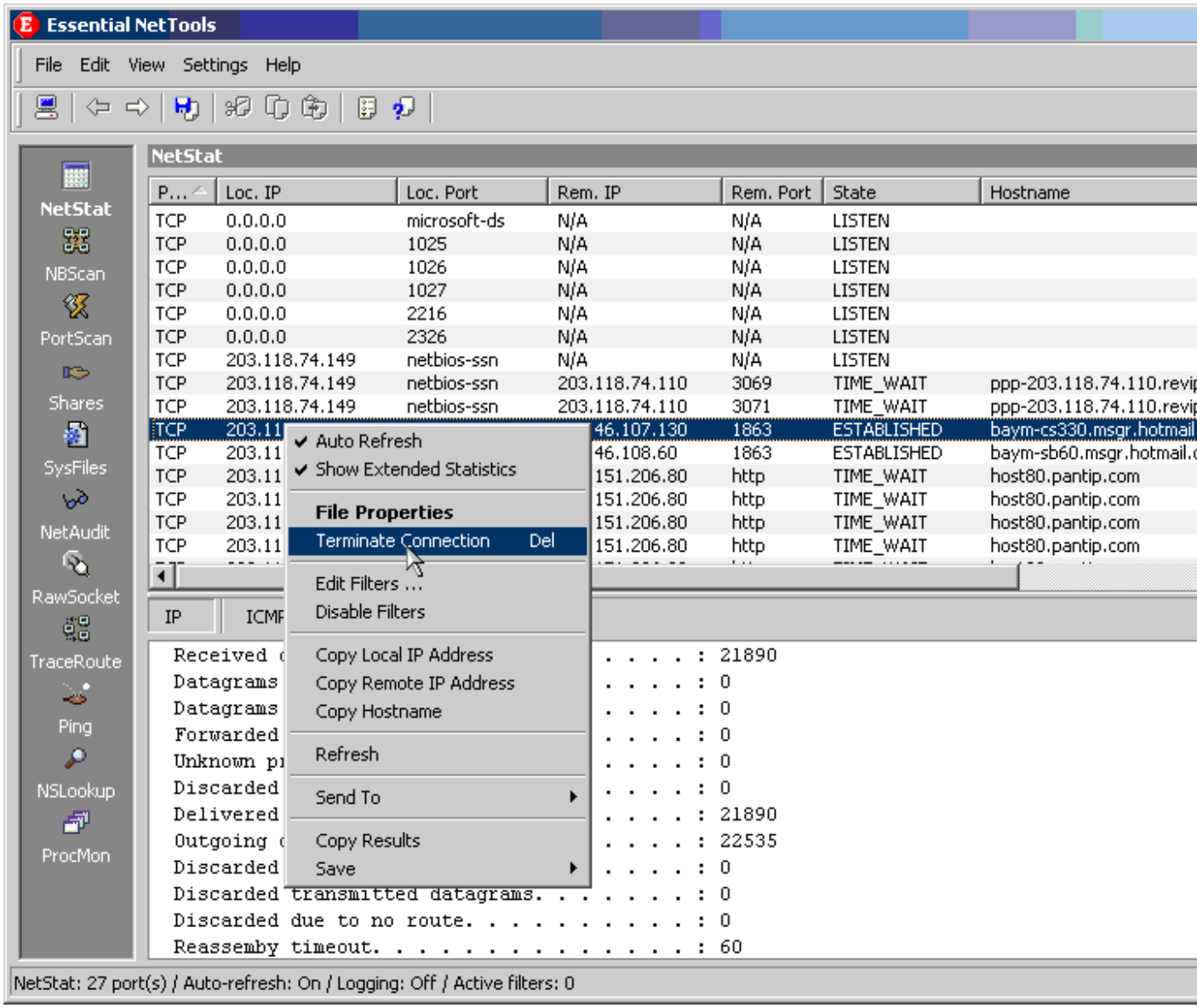
หา download ได้ที่ http://www.web-hack.ru/download/info.php?go=4



1. เมื่อเรียกโปรแกรมมาให้กดที่ วงกลมเลข 1 เพื่อเป็นการเรียกโปรแกรม netstat การแสดงผลจะเหมือนโปรแกรม netstat
2. เลข IP เครื่องที่กำลังรันโปรแกรมนี้เราเอง
3. Port ที่เครื่องนี้ได้เปิดอยู่
4. เลข IP เครื่องอื่นๆที่เข้ามาติดต่อกับเครื่องที่กำลังรันโปรแกรมนี้ คือเครื่องที่มา hackเรา หรือเป็น IP เว็บต่างๆที่คุณได้เข้าอยู่
5. port ที่เครื่องอื่นๆเปิด เพื่อจะมาติดต่อกับเครื่องเรา หรือเครื่องที่กำลังรันโปรแกรม นี้
6. เป็นสถานะการติดต่อ
7. เหมือนกับข้อ 4 แต่อันนี้จะเป็นชื่อเครื่องนั้น หรือเว็บที่เราเปิดอยู่ โดยชื่อนี้จะแทน IP ก็ได้เหมือนเวลาพิมพ์เข้าเว็บต่างๆ

ขอข้ามขั้นตอนก่อน ต่อจากข้างบน (เครื่องโดน hack) ถ้ามีเครื่องอื่นที่เข้ามาเราสามารถยกเลิกการติดต่อได้โดย คลิกขวาที่บรรทัดที่คุณสงสัยว่า ip นั้นเข้ามาละเมิดเครื่องคุณ และทำตามรูปข้างล่างนี้ ซึ่งการที่คุณจะสามารถเอาเครื่องที่เชื่อมต่อกับคุณ (hackเราอยู่) ซึ่งสงสัยว่าใช่แน่ๆ จากรูปด้านล่างนี้ มีเครื่องที่มี IP 203.18.74.110 ได้กำลังแสกนเครื่องนี้ที่ Port 139 หรือ netbios-ssn อยู่ เรารู้ได้เราะว่าสถานะที่ State = TIME_WAIT

แต่ถ้าสถานะที่ State = ESTABLISHED หมายถึง ได้มีการเชื่อมต่อที่สมบูรณ์แล้ว คืออาจมีการ รับ/ส่งไฟล์ หรือ โดน hack อยู่ก็เป็นได้เราสามารถที่จะคลิกขวาที่บรรทัดนั้น แล้วเลือก Terminate Conneciton Del เพื่อเป็นการยกเลิกการเชื่อมต่อ ระหว่างเครื่องคุณ กับเครื่องนั้นๆ แต่ตัวอย่างที่ทำให้ดูนั้นเป็น Port การเชื่อมต่อของ MSN (การยกเลิกเชื่อมต่อนั้น สถานะที่ State = ESTABLISHED เท่านั้น ถึงจะทำได้)



การหาโปรแกรมที่เปิด Port

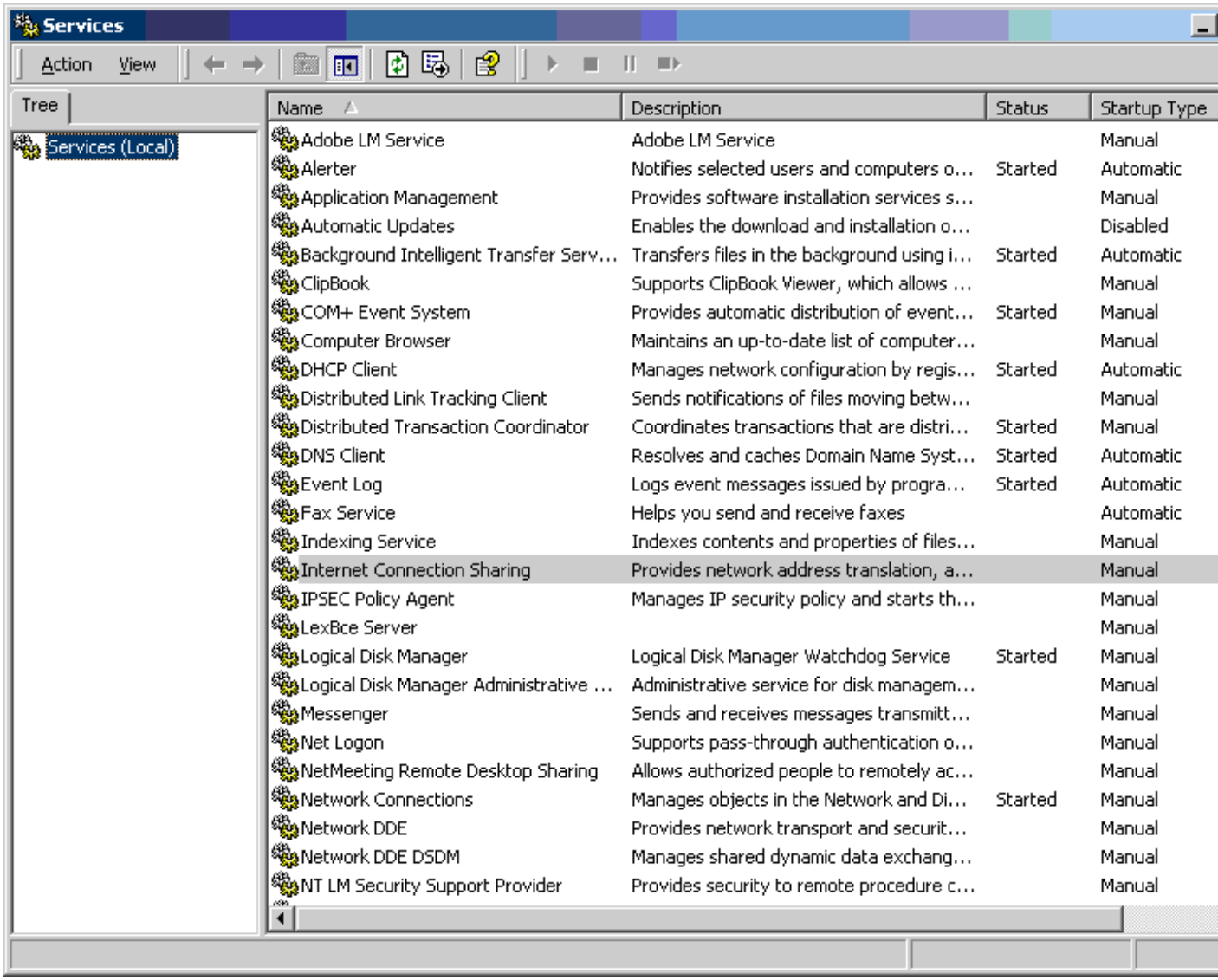
เมื่อคุณทราบว่าเครื่องได้มีการเปิด Portเราไม่ต้องการให้เปิด อาจเป็นพวกโปรแกรมโทรจัน ต่างๆที่แอบเข้ามาเปิด ซึ่งคุณสามารถหาที่อยู่โปรแกรมได้โดย คลิกขวาที่บรรทัดที่มีการเปิด Portเราคิดว่าเป็น โทรจันเราต้องการที่จะปิด Port นั้นๆ และเลือก File Properties หรืออาจเลื่อน tab ด้านล่างของหน้าต่างบน ไปทางขวาแล้วดูตรง ช่องขวาสุด (ดูจากรูปบนนี้นะคับ แต่เลือกอีกอัน)โปรแกรมจะบอกว่า ไฟล์อะไรและอยู่ที่ไหนที่ทำให้เปิด Port นั้นๆแล้วตามไปลบได้เลยครับ

แต่ถ้าจะให้ดีเราต้องมีความรู้เกี่ยวกับการใช้ regeditเราจะต้องไปหา KEY-VALUE-DATAใน regedit เป็นการถอนรากถอนโคน โปรแกรมที่มาเปิด Port เครื่องของคุณซึ่งผมจะขอเอาข้อความใน Pantip ที่เคยได้โพสในกระทู้ แต่ถ้าแค่เอาออกเฉยๆ

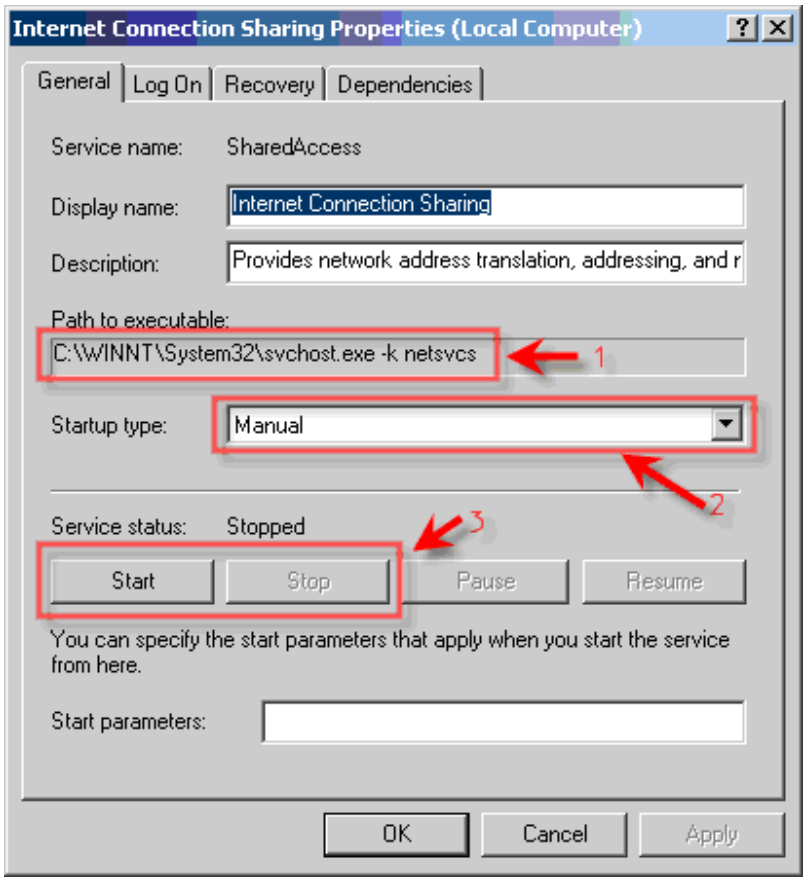
start >> run พิม regdit กด enter
โปรแกรม โทรจัน ส่วนใหญ่มันจะอยู่ที่ Registry ตามข้างล่างนี้ครับ ให้ลองไปหาดูที่นี่ก็ได้
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Runonce
มันจะมีตัวแปร Value ทางด้านขวามือ เพื่อที่จะเรียกโปรแกรมโทรจัน ลบได้เลยครับ แต่ถ้าคุณอยากที่จะหาแบบละเอียด เอาให้หมดจด ก็วิธีด้านล่างนี่เลยครับ

ไปที่เมนู edit >> find จะมีหน้าต่างค้นหาขึ้นมา ติ๊กเครื่องหมายถูกให้หมดนะครับ จากนั้น พิม "ชื่อไฟล์ที่ได้เปิด Port " (ไม่ต้องใส่ฟันหนูนะ) แล้วกดปุ่ม find เมื่อเจอคุณสามารถที่จะลบได้เลย แต่ส่วนใหญ่จะอยู่หน้าต่างด้านขวาของโปรแกรม regedit ซึ่งเป็นตัว data ใช้ในการรันโปรแกรม (ถ้าคุณแน่ใจว่าเป็นโทรจันจริงๆ ลบได้เลย) จากนั้นให้คุณไป search/find ในไดร์ว C,D ของคุณต่อไปว่าไฟล์ที่ว่านั้นได้เก็บอยู่ที่ไหน ให้ตามไปลบอีกที

แต่ยังอยากเก็บโปรแกรมที่ว่าอยู่ให้ start >> run พิม msconfig แล้วคุณหาเมนู Tab StartUp และหาโปรแกรมที่ว่าในนั้น พอเจอแล้วเอาเครื่องหมายถูกหน้าโปรแกรมที่ว่าออก
คำเตือน ในการที่จะลบเราจำเป็นต้องเข้าใจว่า ตรงที่ๆคุณได้เจอนั้นลบไปแล้วจะไม่เกิดปัญหาที่จะตามมาทีหลัง เพราะบางทีอาจทำให้เครื่องมีปัญหาตามมาทีหลังเราอาจปล่อยทิ้งไว้ก็ได้ ต้องแน่ใจจริงๆว่าที่คุณได้ลบไป เป็นโปรแกรมที่คุณไม่ต้องการให้รันมาทุกครั้ง (โทรจัน) เมื่อตอนคุณบูทเครื่อง
เมื่อได้ลบใน REGISTRY ไปแล้วค่อยตามไปลบในไดรว์ที่คุณเจอตามปรกติ ซึ่งโปรแกรมได้บอกที่อยู่ของไฟล์มาแล้ว จากที่อธิบายมาข้างบนเราอาจไปปิด Serviceเราได้เปิด โดยการ ไปที่
Start > Run พิมพ์ Services.msc ; ใช้ได้กับ Win200/XP จะมีหน้าต่างขึ้นมาดังรูปข้างล่างนี้ ส่วน Win 98/meเราแค่ตามไปลบที่อยู่ของไฟล์กับที่ REGISTRY



ทางหน้าต่างด้านขวานั้น เป็นตัวที่เปิด/ปิด Service ต่างๆ และมีคำอธิบายต่างๆอยู่แล้ว พร้อมทั้งมีการบอกสถานะต่างๆด้วยว่าได้ทำงานแบบใด(Auto-Manual-Disadle) กำลังทำอยู่หรือไม่(Start-หรือเป็นช่องว่างๆ) สามารถที่จะกำหนดได้ว่าจะให้เป็นแบบไหน แต่ผมแนะว่าถ้าไม่แน่ใจใน Service นั้นๆที่คุณสงสัย ให้กำหนดการทำงาน Service เป็นแบบ Manual จะดีกว่า และคุณต้องเข้าไปดูในแต่ละ Service เองแต่ละตัว ก็คือพวกโปรแกรมที่เปิด Port ซึ่งต้อง ดับเบิ้ลคลิกเข้าไป ว่ามีโปรแกรมไหนเปิดบริการ แชร์ต่างๆ ที่ไม่จำเป็น ให้เอาออกได้ แต่คุณต้องระวังให้ดี บางอย่างถ้าคุณเอาออกไป เครื่องอาจมีอาการแปลกๆก็ได้ครับ ทางที่ดีควรจดไว้ทุกครั้งว่า ค่าเดิมเป็นอย่างไร และ เปลี่ยนอะไรไปบ้าง และทุก Service ที่เห็นในนั้น เมื่อคุณ เบิ้ลคลิกเข้าไป จะมีหน้าต่างขึ้นมา มันจะบอกว่าเป็นไฟล์อะไรที่รัน Service รวมทั้ง Option ด้วย ดังรูป



ตรงเลข 1 จะบอกไฟล์ที่รัน Service ตัวนั้นๆ พร้อมทั้ง Option ต่างๆ ที่ได้รันขึ้นมาเมื่อคุณบูทเครื่อง ตรงนี้อยากให้ทุกท่านได้เปิดดูโปรแกรม Essential NetTools ไปด้วย ว่าตรงกับ Port ไหน

ตรงเลข 2 จะเป็นการกำหนดให้ Service ตัวนั้นๆทำงานแบบไหน ถ้าเป็นเรื่องเกี่ยวกับ Port ไม่ควรให้เป็นแบบ Auto ควรจะตั้งให้เป็นแบบ Manual จะดีกว่าเราสามารถที่จะเรียกขึ้นมาก็ได้ แต่ถ้าคุณไม่เรียก Service นั้นก็ไม่ทำงาน และคุณสามารถยกเลิกได้ด้วยเมื่อเลือก Disable

ตรงเลข 3 ต่อจากเลข 2 นิดๆเราจะเลือก Disable Service ตัวนั้นๆเราไม่ต้องการให้มันรับขึ้นมาตอนบูทเครื่อง (เปิด Port) ให้คุณลองกดปุ่ม Stop เพื่อเป็นการทดสอบดูก่อน ว่ามีผมกระทบแบบไหน เมื่อเราได้ปิด Service ตัวนั้นๆ ถ้าไม่มีปัญหาใดๆเกิดขึ้น ค่อยไป Disable Service ตัวนั้นๆ ตามหมายเลข2 ที่ได้ชี้

การ SETUP เกี่ยวกับ netstat ในโปรแกรม Essential NetTools

โดยปรกติแล้ว ถ้าคุณใช้โปรแกรมในดอส netstat -an เพื่อดูการเชื่อมต่อใน Internet ระหว่าเครื่องคุณกับเครื่องอื่นๆเราจะต้องคอยพิมพ์ไปเรื่อยๆ ด้วยคำสั่งเดิมซ้ำ เพื่อดูการเชื่อมต่อที่ update ตลอดเวลา แต่โปรแกรม netstat ในโปรแกรม Essential

NetTools จะมีการ update ทุกๆ 5 วินาทีซึ่งเป็นข้อดีของโปรแกรมนี้ สามารถที่จะเปลี่ยนเวลาให้เร็ว/ช้าได้ เป็น วินาที ตามที่คุณต้องการ และการเซ็ทค่าอื่นๆ ในโปรแกรม เพื่อให้ง่ายต่อการเข้าใจ ดังรูปด้านล่างนี้ ก่อนอื่นให้ทำตามนี้ก่อน(ไปที่เมนู Settings > Option..)