



The Wonderful World of Services

By: Stefanja



What Is a Service?

- Make the computer world go round
 - Without Services we'd have nothing
- A service is an application that runs in the background to enable a computer to do certain thing.
 - Ex: SSH, DNS, DB, AD, HTTP, IMAP, FTP
 - Who does not know what these things are???

*You guys should have tons of service experience from your homeworks and learning how to set them up



Service Names

- Depends on what application you are using to run a specified service.
 - Apache ,IIS or Nginx → Web
 - Mariadb Or MySQL → DB
- Some services can only be run by one application.
 - Windows Active Directory → AD



Know Your Ports

- Services use different ports
 - HTTP → 80 / 8080
 - DNS → 53
 - SSH → 22
- Common security practice to change these to non standard ports
 - Makes it harder for attackers to find, etc.

Well-Known Port Numbers



Service, Protocol, or Application	Port Number	TCP or UDP
FTP (File Transfer Protocol)	20, 21	TCP
SSH (Secure Shell Protocol)	22	TCP
Telnet	23	TCP
SMTP (Simple Mail Transfer Protocol)	25	TCP
DNS (Domain Name System)	53	UDP
TFTP	68	UDP
HTTP	80	TCP
POP3	110	TCP
IMAP4	143	TCP
HTTPS	443	TCP

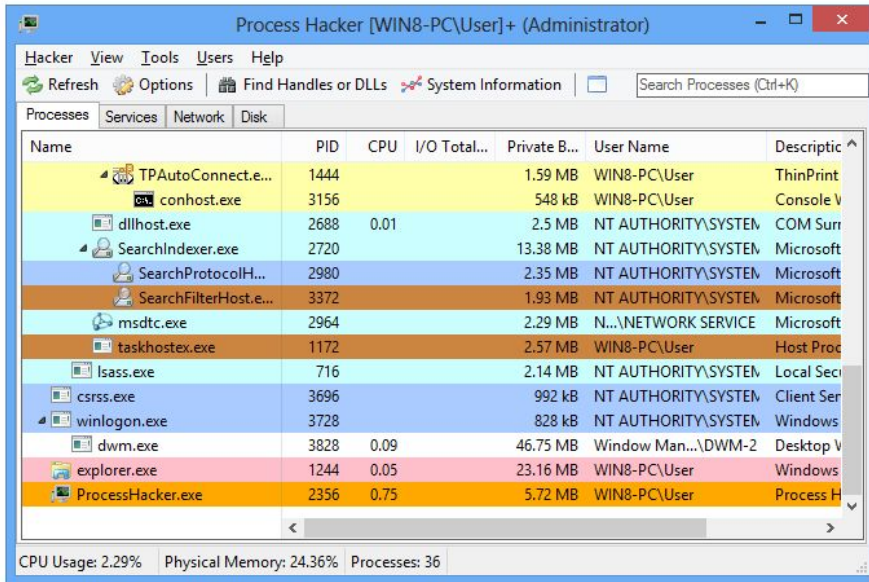


How Do I find Windows Services?

- ANY Windows
 - Task Manager - resource usage
 - Ctrl + Alt + Del or right click on taskbar or windows + x
 - Services.msc - shows running services
 - CMD → services.msc
 - Windows search for services

Etc. Windows Services tools

A detailed overview of system activity with highlighting.



Name	PID	CPU	I/O Total...	Private B...	User Name	Descriptio
TPAutoConnect.e...	1444			1.59 MB	WIN8-PC\User	ThinPrint
conhost.exe	3156			548 kB	WIN8-PC\User	Console V
dllhost.exe	2688	0.01		2.5 MB	NT AUTHORITY\SYSTEM	COM Sur
SearchIndexer.exe	2720			13.38 MB	NT AUTHORITY\SYSTEM	Microsoft
SearchProtocolH...	2980			2.35 MB	NT AUTHORITY\SYSTEM	Microsoft
SearchFilterHost.e...	3372			1.93 MB	NT AUTHORITY\SYSTEM	Microsoft
msdtc.exe	2964			2.29 MB	N...\NETWORK SERVICE	Microsoft
taskhost.exe	1172			2.57 MB	WIN8-PC\User	Host Proc
lsass.exe	716			2.14 MB	NT AUTHORITY\SYSTEM	Local Sec
csrss.exe	3696			992 kB	NT AUTHORITY\SYSTEM	Client Ser
winlogon.exe	3728			828 kB	NT AUTHORITY\SYSTEM	Windows
dwm.exe	3828	0.09		46.75 MB	Window Man...\DWM-2	Desktop V
explorer.exe	1244	0.05		23.16 MB	WIN8-PC\User	Windows
ProcessHacker.exe	2356	0.75		5.72 MB	WIN8-PC\User	Process H

CPU Usage: 2.29% | Physical Memory: 24.36% | Processes: 36

Graphs and statistics allow you quickly to track down resource hogs and runaway processes.

- Process Hacker- Similar tool to Task Manager
- Needs to be installed
- Jered's Fav tool

<http://processhacker.sourceforge.net/>



How Do I find Stop or Start Windows Services?

- Services.msc
 - Right click on service → start, stop, restart
- **BEWARE:** Windows services have dependencies!!
 - Ex: Windows Firewall service depends on Base Filtering Engine
 - Dependencies tab of service properties
 - Some May not start or stop if dep. is broken



- Major Windows service
 - Extremely dependent on DNS
 - If your Active directory is broken
 - Check DNS, It's probably DNS...
 - It's DNS
 - Refer to Windows Lecture if you don't know what this is!!



Linux Services

- In Linux, services are applications or processes that run in the Background.
 - They are sometimes referred to as daemons.
 - Many of their names will end with “d” out of convention (e.g. sshd, httpd).



How Do I Find Linux Services?

- ANY Linux
 - Command Line
 - `ps aux` - shows running services
 - `top` - resource usage
 - Interactive and updates every second

Etc. Linux Services tools

```
~/projects/htop
1 [|||||] 34.3% Aug
2 [|||||] 55.0%
3 [|||||] 43.0%
4 [|||||] 47.0%
Mem [|||||] 1.16G/7.81G Tasks: 55, 165 thr: 3 running
Sup [|||||] 0K/0K Load average: 0.64 0.38 0.29
Uptime: 05:19:59
Battery: 35.5% (Running on AC)

PID USER PRI NI VIRT RES SHR CPU% MEM% TIME+ Command
5177 hisham 20 0 35020 5000 4592 S 0.0 0.1 0:00.00 | gmain
5176 hisham 20 0 2952 2080 1976 S 0.0 0.0 0:00.05 | /bin/dbus-daemon --conf ig-file=/System/Settings/at-spi2/ac
5175 hisham 20 0 35020 5000 4592 S 0.0 0.1 0:00.00 | gdbus
5168 root 20 0 34456 6224 5236 S 0.0 0.1 0:02.90 | /usr/lib/upower/upowerd
5170 root 20 0 34456 6224 5236 S 0.0 0.1 0:00.00 | gdbus
5169 root 20 0 34456 6224 5236 S 0.0 0.1 0:00.00 | gmain
5165 hisham 20 0 177M 12896 6764 S 0.0 0.2 0:47.75 | /usr/bin/pulseaudio --start --log-target=syslog
5309 hisham 20 0 177M 12896 6764 S 0.0 0.2 0:00.00 | | aalsa-source-ALC
5308 hisham 20 0 177M 12896 6764 S 0.0 0.2 0:00.00 | | aalsa-sink-ALC36
5180 hisham 20 0 177M 12896 6764 S 0.0 0.2 0:00.01 | | aalsa-source-ALC
5174 hisham 20 0 177M 12896 6764 S 0.0 0.2 0:45.67 | | aalsa-sink-ALC36
5160 hisham 20 0 32288 11616 10624 S 0.7 0.1 0:00.67 | xfsetts ingstd
5167 hisham 20 0 32288 11616 10624 S 0.0 0.1 0:00.53 | | gmain
5159 hisham 20 0 35076 17196 14320 S 0.0 0.2 0:01.17 | xfce4-power-manager
5161 hisham 20 0 35076 17196 14320 S 0.0 0.2 0:00.00 | | gdbus
5150 hisham 20 0 64348 31912 22820 S 0.0 0.4 0:00.68 | nm-applet
5207 hisham 20 0 64348 31912 22820 S 0.0 0.4 0:00.00 | | gdbus
5146 hisham 20 0 46952 22548 16712 S 0.0 0.3 0:01.52 | xfdesktop
5211 hisham 20 0 46952 22548 16712 S 0.0 0.3 0:00.53 | | gmain
5144 hisham 20 0 33156 13072 12216 S 0.0 0.2 0:00.02 | Thunar --daemon
5153 hisham 20 0 33156 13072 12216 S 0.0 0.2 0:00.00 | | gmain
5142 hisham 20 0 39672 21724 17000 S 0.0 0.3 0:04.26 | xfce4-panel
19006 hisham 20 0 18388 8600 7012 S 0.0 0.1 0:00.14 | | urxvt -cr green -fn *-lode-* -fb *-lode-* -fi *-lode-* -fb
19007 hisham 20 0 8788 5088 3700 S 0.0 0.1 0:00.09 | | zsh
F1 Help F2 Setup F3 Search F4 Filter F5 Sorted F6 Collap F7 Nice F8 Nice F9 Kill F10 Quit
```

- htop- Similar tool to Process Hacker
- Needs to be installed
 - <package manager> install htop
- Vince's Fav tool

<http://hisham.hm/htop/>



How Stop Linux Services?

- To ask a process to terminate (but it could choose to ignore you):
 - `$ kill <pid>`
- To force the kernel to kill a process (this cannot be ignored):
 - `$ kill -9 <pid>`
 - `$ kill -KILL <pid>`
 - `$ kill -SIGKILL <pid>`

*Pid = Process ID



How Control Linux SystemV Services?

- System V (Aka. SysV)
 - Older system architecture
 - `# service <name> <start | stop | restart | reload | status >`
 - `# service sshd status`



How Control Linux Systemd Services?

- Systemd
 - # systemctl <start | stop | restart | reload | status >
<name>
 - # systemctl reload nginx



Nmap



- Installation
 - `<package manager> install nmap`
 - Zenmap on windows
- Nmap is an open source port scanner and network recon tool.
 - Install and scan your subnet for computers and services



Nmap Flags

- Nmap <ip address/subnet>
- Nmap -sT -O <ip address /subnet>
- Nmap -sS -sV -O <ip address/subnet>
- Many other flags!!! Nmap to your hearts content
 - [Nmap Flag Cheat Sheet](#)



Nmap Uses

- Red teamers or attackers will scan your subnet to find computers
- Find what's running on certain machines
- This information will tell them what services are there and what type of machine/ server it is.



Services down?

- In a competition setting
 - Red team will bring your services down
 - Linux: simple as → `service/systemctl <name> stop`
 - Windows: Active directory → stop
- Your goal is to keep your services up to keep the business running. Without services we have no business



Summary !!!

- Services are mega important!!!
- Don't let them break/go down
 - If they do fix them
- Know your ports!!
- Know how services work!!
- Monitor, Monitor, Monitor!!!
 - If there are shells that aren't being run by you kill them



LAMP Stack

- Linux - Open source OS
- Apache - Web application to make your machine a Web server
- MySQL - DB App to hold contents of the Web Server
- Php - Programming language used to edit websites.. Etc
- Php plugins is also used by other software such as Wordpress



Installation

- Apache
 - `<package manager> install apache 2`
- MySQL
 - `<package manager> install mysql-server`
- PHP
 - `<package manager> install php, libapache2-mod-php, php-mcrypt, php-mysql`
 - <https://www.digitalocean.com/community/tutorials/how-to-install-linux-apache-mysql-php-lamp-stack-on-ubuntu-16-04>