# 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

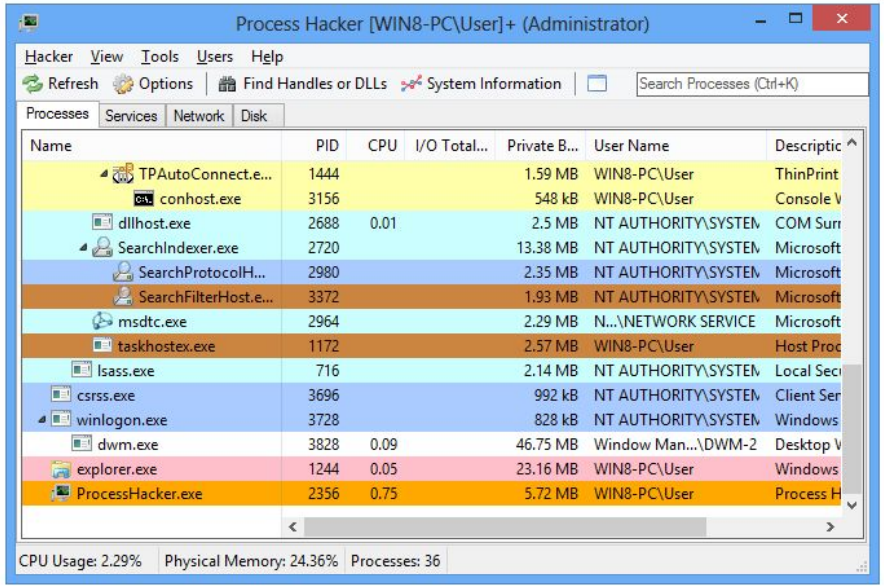
| Service, Protocol, or Application | Port Number | TCP or UDP |
|---|---|---|
| FTP (File Transfer Protocol) | 20, 21 | TCP |
| SSH (Secure Shell Protocol) | 22 | TCP |
| Telnet | 23 | TCP |
| SMTP (Simple Mail Transfer Protocol) | 25 | TCP |
| DNS (Domain Name System | 53 | UDP |
| TFTP | 69 | UDP |
| 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.




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!!

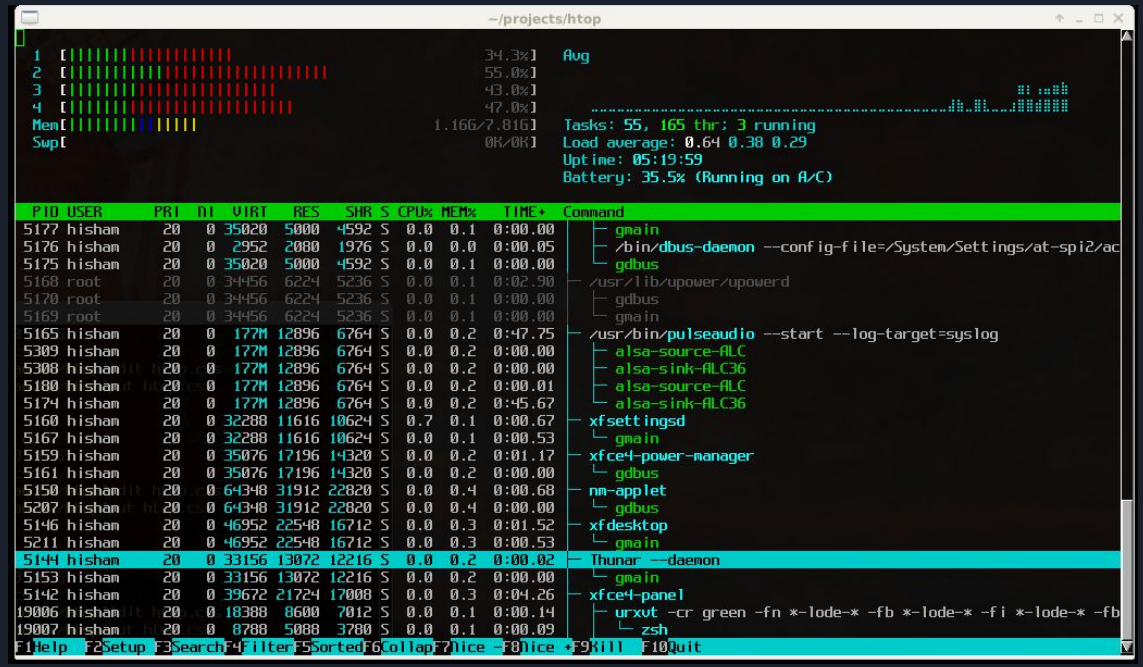
# Linux Services

- 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




- 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