

Services

UBNetDef, Spring 2022
Week 9

Lead Presenters:
Alex Skowronski and Ethan Viapiano

Learning Goals

- Explore the applications of remote and local services
- Initially configured a MySQL database
- Initialize MediaWiki setup
- Utilize application layer network protocols
- Learn how to use network reconnaissance tools

Client vs Server

- Client

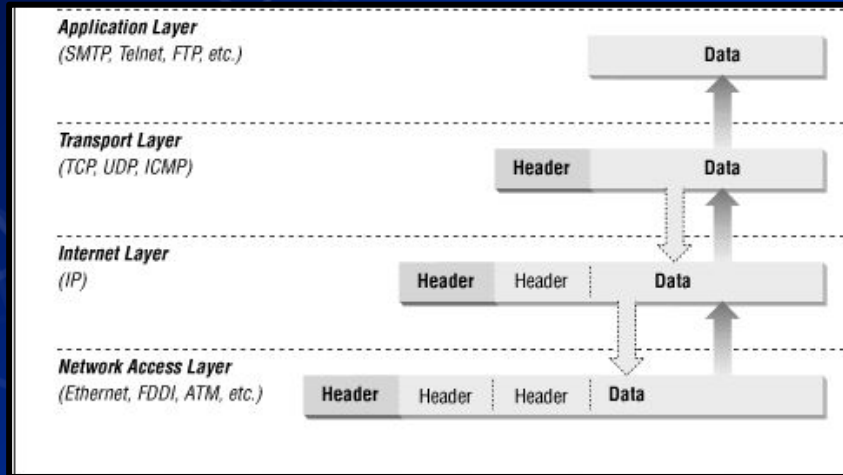
- Runs a bunch of services for a limited amount of users
- Ex: Win10Client, UbuntuClient

- Server

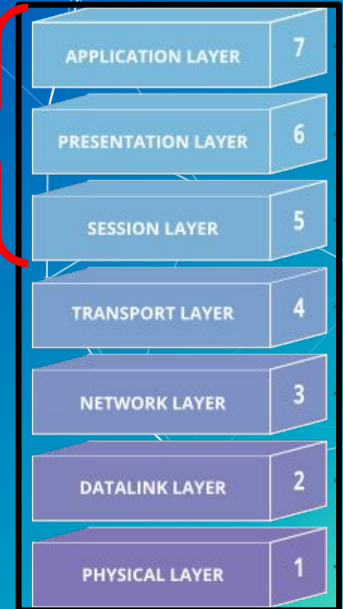
- Runs a limited amount of services for a larger number of users
- Ex: ServerAD (Active Directory), ServerGUI (IIS), UbuntuWebServer (Apache)

Application Layer

- Specifies shared protocols for communication between devices



"Application Layer"



Protocols

- Protocol
 - Set of rules or procedures for transmitting data between devices
- Most protocols have “standard” ports
- What are some protocols you have used in this class?

Types of Protocols

- Domain Name System (DNS)
- Email:
 - Simple Mail Transfer Protocol (SMTP)
 - Post Office Protocol (POP3)
- Remote access:
 - Remote Desktop Protocol (RDP)
 - Secure Shell (SSH)
- File Transfer:
 - File Transfer Protocol (FTP)
 - Secure Copy Protocol (SCP)
- Web:
 - Hypertext Transfer Protocol (HTTP)
 - Hypertext Transfer Protocol Secure (HTTPS)

Port #	Protocol
21	FTP Control
20	FTP Data
23	Telnet
25	SMTP
53	DNS
80	HTTP
110	POP3
143	IMAP
443	HTTPS

Web

- Web Servers process incoming requests from clients to web over protocols
 - Web resources are identified by a **U**niform **R**esource **L**ocator (URL)
- Common protocols
 - **H**yper**T**ext **T**ransfer **P**rotocol (HTTP)
 - Unencrypted communication
 - Port 80
 - **H**yper**T**ext **T**ransfer **P**rotocol **S**ecure (HTTPS)
 - Encrypted communication
 - Client is able to authenticate the server
 - Port 443

How we get to our website

- Website: <https://ubnetdef.org/>
- Get an IP address, gateway, etc.
- Resolve "ubnetdef.org" to an IP address
- Send an HTTP GET request to 128.205.44.157 asking for host ubnetdef.org and path "/"
- Note that the above steps are simplified: a lot more happens

Recall SSH

- SSH is a remote access protocol for encrypted client-server connection.
- Access is provided to the shell through a command line interface.
- The common port for SSH is 22.

```
sysadmin@ubuntu-client:~$ ssh admin@10.1.1.1
Password for admin@pfSense.home.arpa:
VirtualBox Virtual Machine - Netgate Device ID: 1b4ee00425120773dac8

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4: 192.168.1.1/24
LAN (lan)      -> em1      -> v4: 10.1.1.1/24

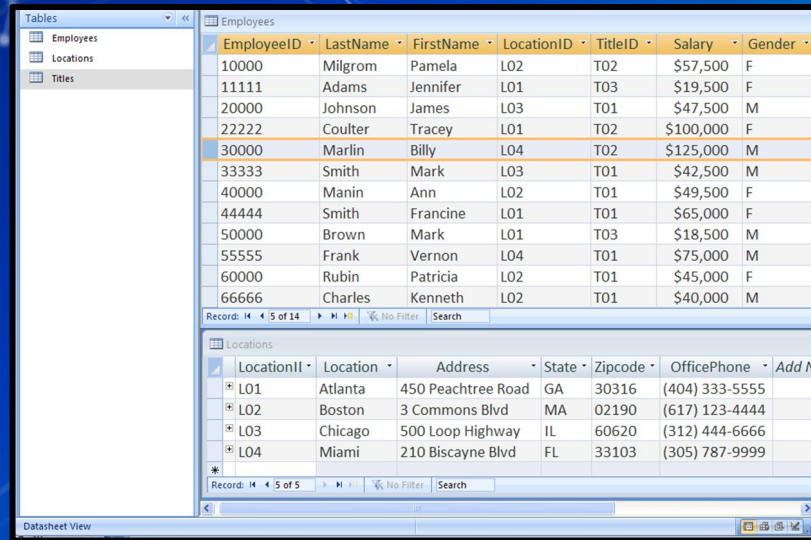
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update from console
5) Reboot system              14) Disable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: 8

[2.6.0-RELEASE][admin@pfSense.home.arpa]/root: whoami
root
[2.6.0-RELEASE][admin@pfSense.home.arpa]/root: █
```

Why databases?

- Collection of data that allows access, retrieval and use of that data
 - Phone book, filing cabinet
 - SQLite, MySQL, Oracle, Microsoft SQL Server, Microsoft Access, MariaDB
- Store structured data in tables made of fields (columns) and records (rows)



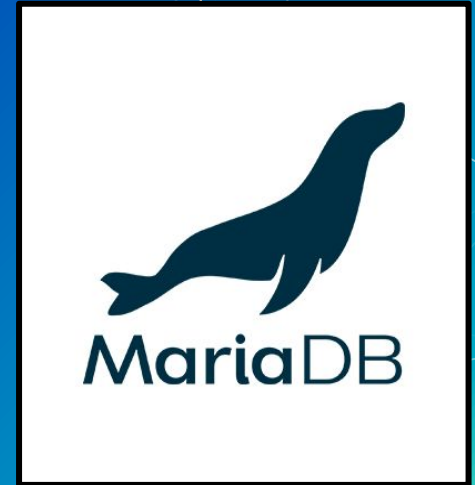
The screenshot shows a database application interface with two tables displayed in a datasheet view. The 'Employees' table is at the top, and the 'Locations' table is at the bottom. Both tables have columns for ID, Name, Location, Title, Salary, and Gender (for Employees) or Location ID, Location, Address, State, Zipcode, and OfficePhone (for Locations). The 'Employees' table has 14 records, and the 'Locations' table has 5 records.

EmployeeID	LastName	FirstName	LocationID	TitleID	Salary	Gender
10000	Milgrom	Pamela	L02	T02	\$57,500	F
11111	Adams	Jennifer	L01	T03	\$19,500	F
20000	Johnson	James	L03	T01	\$47,500	M
22222	Coulter	Tracey	L01	T02	\$100,000	F
30000	Marlin	Billy	L04	T02	\$125,000	M
33333	Smith	Mark	L03	T01	\$42,500	M
40000	Manin	Ann	L02	T01	\$49,500	F
44444	Smith	Francine	L01	T01	\$65,000	F
50000	Brown	Mark	L01	T03	\$18,500	M
55555	Frank	Vernon	L04	T01	\$75,000	M
60000	Rubin	Patricia	L02	T01	\$45,000	F
66666	Charles	Kenneth	L02	T01	\$40,000	M

LocationID	Location	Address	State	Zipcode	OfficePhone	Add N
L01	Atlanta	450 Peachtree Road	GA	30316	(404) 333-5555	
L02	Boston	3 Commons Blvd	MA	02190	(617) 123-4444	
L03	Chicago	500 Loop Highway	IL	60620	(312) 444-6666	
L04	Miami	210 Biscayne Blvd	FL	33103	(305) 787-9999	

MariaDB

- Database client and server software
- Relational database management system (DBMS)
- Used as a backend database for many web applications.
 - MediaWiki
 - WordPress
 - Wiki.js



In Class Demo

Using MariaDB

MariaDB Demo

- ⬡ Command Line Interface (CLI)
- ⬡ Logging in
 - ⬢ `sudo mysql -u root -p`
- ⬡ List all available databases
 - ⬢ `SHOW DATABASES;`
- ⬡ Interact with specific database
 - ⬢ `USE <DATABASE NAME>;`
- ⬡ Show all available tables
 - ⬢ `SHOW TABLES;`
- ⬡ Show all values in a table
 - ⬢ `SELECT * FROM <TABLE NAME>;`



QUESTIONS?

In Class Activity

RockyDBServer Setup

RockyDBServer Setup

- ⬡ Database Setup on [RockyDBServer](#):
 - ⬡ Use netstat to check if SQL is running, It's on port 3306
 - `ss -tlp`
 - ⬡ Check the Status of MariaDB
 - `sudo systemctl status mariadb`
 - ⬡ Start the MariaDB Service if necessary
 - `sudo systemctl start mariadb`
 - ⬡ Enable the Service for Automatic Start
 - `sudo systemctl enable mariadb`
 - ⬡ Verify that MariaDB is enabled and running
 - `sudo systemctl status mariadb`

RockyDBServer Setup

Database Setup on [RockyDBServer](#):

- ⬡ Improve the security of MariaDB
 - ⬡ `mysql_secure_installation`
- ⬡ Verify that MariaDB is listening on the correct port
 - ⬡ `ss -tlp`
- ⬡ Verify that the Public Zone is currently active on your RockyDBServer firewall
 - ⬡ `sudo firewall-cmd --get-active-zones`
- ⬡ Permanently whitelist the port in the “public” zone in your RockyDBServer Firewall
 - ⬡ `sudo firewall-cmd --permanent --zone=public --add-port=3306/tcp`

Break

Please return in 10 minutes

What is a Wiki?

- Web resource curated by its own audience using a web browser.
- Service requirements of a wiki
 - Web server
 - Database server



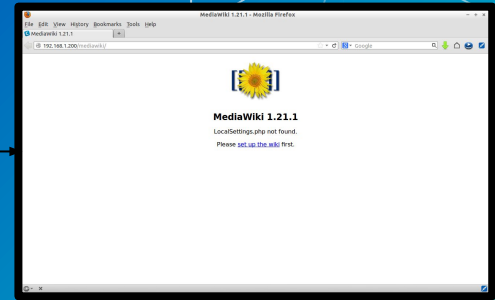
Database

Serves:
Database Info



Web Server

Serves:
Dynamic Webpage



Client

In Class Activity

Web Server Setup

Web Server Setup

Web Server Setup on **UbuntuWebServer**:

- ⬡ Move to tmp directory
 - ⬡ `cd /tmp`
- ⬡ Use `wget` to download **MediaWiki**
 - ⬡ `wget`
<https://releases.wikimedia.org/mediawiki/1.36/mediawiki-1.36.2.tar.gz>
- ⬡ Extract the archive
 - ⬡ `tar -xvzf /tmp/mediawiki-1.36.2.tar.gz`
- ⬡ Make a mediawiki directory
 - ⬡ `sudo mkdir /var/lib/mediawiki`
- ⬡ Move the contents of the extracted mediawiki to `/var/lib/mediawiki`
 - ⬡ `sudo mv mediawiki-1.36.2/* /var/lib/mediawiki`

Recall Services And Processes

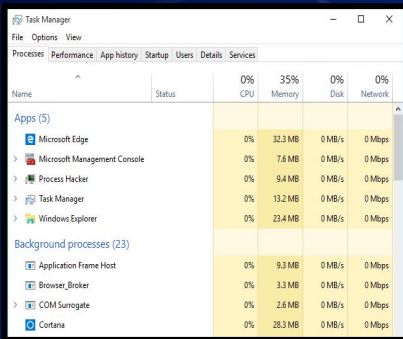
- Services and Processes

- Common processes are instances of a program
 - Often initiated and terminated by user action
 - notepad.exe, mspaint.exe, Rocket League
- Active services are persistent processes
 - Often run in the background
 - Xbox Live Game Service, Windows Update manager
- Services are known to the OS whether they are running or not

- Typically manage things that make the system work

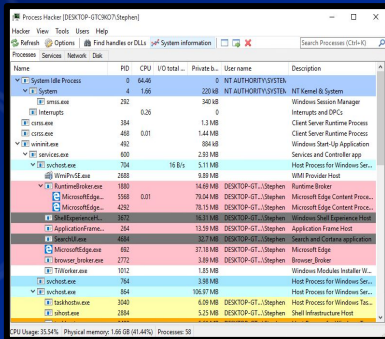
How can I see my machine's processes?

■ Process Managers:



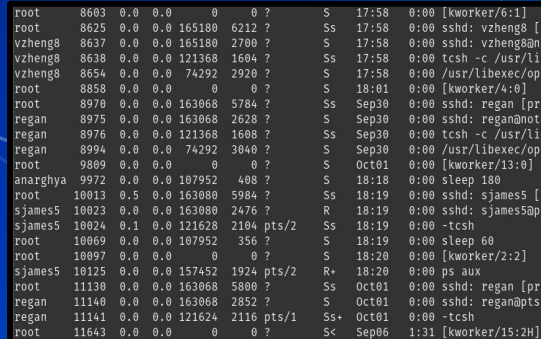
The screenshot shows the Windows Task Manager interface. The 'Processes' tab is selected, displaying a list of running applications and background processes. The columns include Name, Status, CPU usage, Memory usage, Disk usage, and Network usage. Applications like Microsoft Edge, Microsoft Management Console, Process Hacker, Task Manager, and Windows Explorer are listed. Background processes include Application Frame Host, Browser_Broker, COM Surrogate, and Cortana.

Name	Status	0% CPU	35% Memory	0% Disk	0% Network
Microsoft Edge	Running	0%	32.3 MB	0 MB/s	0 Mbps
Microsoft Management Console	Running	0%	7.6 MB	0 MB/s	0 Mbps
Process Hacker	Running	0%	9.4 MB	0 MB/s	0 Mbps
Task Manager	Running	0%	13.2 MB	0 MB/s	0 Mbps
Windows Explorer	Running	0%	23.4 MB	0 MB/s	0 Mbps
Background processes (23)					
Application Frame Host	Running	0%	9.3 MB	0 MB/s	0 Mbps
Browser_Broker	Running	0%	3.3 MB	0 MB/s	0 Mbps
COM Surrogate	Running	0%	2.6 MB	0 MB/s	0 Mbps
Cortana	Running	0%	28.3 MB	0 MB/s	0 Mbps



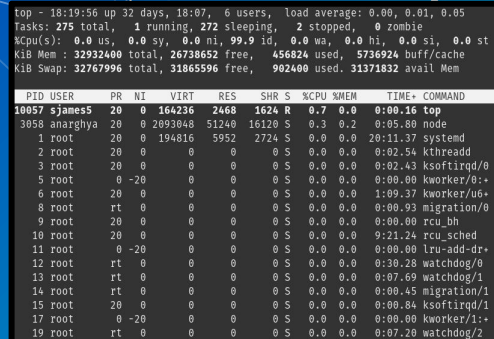
The screenshot shows the Process Hacker application. It displays a detailed list of system processes, including their PID, CPU usage, I/O total, Private bytes, User name, and Description. Processes like System Idle Process, System, smss.exe, csrss.exe, and various system services are visible.

Name	PID	CPU	I/O total	Private	User name	Description
System Idle Process	0	0.00	0	0	NT AUTHORITY\SYSTEM	
System	4	0.00	220 KB	0	NT AUTHORITY\SYSTEM	NT Kernel & System
smss.exe	292	0.00	340 KB	0		Windows Session Manager
csrss.exe	384	0.00	1.3 MB	0		Client Server Runtime Process
csrss.exe	488	0.01	1.44 MB	0		Client Server Runtime Process
svchost.exe	492	0.00	884 KB	0		Windows Start-Up Application
svchost.exe	800	0.00	2.93 MB	0		Service and Controller app
svchost.exe	704	0.00	16 B/s	5.11 MB		Host Process for Windows Ser...
Winlogon.exe	388	0.00	3.93 MB	0		UMW Provider Host
RuntimeBroker.exe	1580	0.00	14.69 MB	0	DESKTOP-GT...Stephen	Runtime Broker
MicrosoftEdge.exe	598	0.01	76.04 MB	0	DESKTOP-GT...Stephen	Microsoft Edge Content Process
MicrosoftEdge.exe	432	0.00	78.15 MB	0	DESKTOP-GT...Stephen	Microsoft Edge Content Process
svchost.exe	700	0.00	16.93 MB	0	DESKTOP-GT...Stephen	Windows Start-Up Application
ApplicationFrameHost.exe	354	0.00	13.59 MB	0	DESKTOP-GT...Stephen	Application Frame Host
svchost.exe	488	0.00	32.78 MB	0	DESKTOP-GT...Stephen	Search and Content application
MicrosoftEdge.exe	880	0.00	37.18 MB	0	DESKTOP-GT...Stephen	Microsoft Edge
browser_broker.exe	2772	0.00	3.89 MB	0	DESKTOP-GT...Stephen	Browser_Broker
svchost.exe	704	0.00	3.88 MB	0	DESKTOP-GT...Stephen	Host Process for Windows Ser...
TaskHost.exe	1072	0.00	1.83 MB	0	DESKTOP-GT...Stephen	Windows Modules Installer W...
svchost.exe	704	0.00	106.97 MB	0	DESKTOP-GT...Stephen	Host Process for Windows Ser...
TaskHost.exe	3840	0.00	6.99 MB	0	DESKTOP-GT...Stephen	Host Process for Windows Tac...
svchost.exe	2884	0.00	5.23 MB	0	DESKTOP-GT...Stephen	Shell Infrastructure Host



The screenshot shows the output of the 'ps -aux' command in a terminal window. It lists all running processes on the system, including their PID, PPID, CPU usage, memory usage, and command line. Processes like [kworker/6:1], sshd: vzheng8, and various user processes are visible.

USER	PID	PPID	CPU	MEM	VSZ	STAT	TIME	COMMAND
root	8603	0.00	0.00	0	0	?	17:58	0:00 [kworker/6:1]
root	8625	0.00	0.00	165180	6212	?	17:58	0:00 sshd: vzheng8 [
vzheng8	8637	0.00	0.00	165180	2700	?	17:58	0:00 sshd: vzheng8an
vzheng8	8638	0.00	0.00	121368	1604	?	17:58	0:00 tcsh -c /usr/li
vzheng8	8654	0.00	0.00	74292	2920	?	17:58	0:00 /usr/libexec/op
root	8858	0.00	0.00	0	0	?	18:01	0:00 [kworker/4:0]
root	8970	0.00	0.00	163068	5784	?	Sep30	0:00 sshd: regan [pr
regan	8975	0.00	0.00	163068	2628	?	Sep30	0:00 sshd: regan@not
regan	8976	0.00	0.00	121368	1608	?	Sep30	0:00 tcsh -c /usr/li
regan	8994	0.00	0.00	74292	3040	?	Sep30	0:00 /usr/libexec/op
root	9809	0.00	0.00	0	0	?	Oct01	0:00 [kworker/13:0]
anarghya	9972	0.00	0.00	107952	408	?	18:18	0:00 sleep 180
root	10013	0.5	0.00	163080	5984	?	18:19	0:00 sshd: sjames5 [
sjames5	10023	0.00	0.00	163080	2476	?	18:19	0:00 sshd: sjames5@p
sjames5	10024	0.1	0.00	121628	2104	pts/2	18:19	0:00 -tcsh
root	10069	0.00	0.00	107952	356	?	18:19	0:00 sleep 60
root	10097	0.00	0.00	0	0	?	18:20	0:00 [kworker/2:2]
sjames5	10125	0.00	0.00	157452	1924	pts/2	18:20	0:00 ps aux
root	11130	0.00	0.00	163068	5800	?	Oct01	0:00 sshd: regan [pr
regan	11140	0.00	0.00	163068	2852	?	Oct01	0:00 sshd: regan@pts
regan	11141	0.00	0.00	121624	2116	pts/1	Oct01	0:00 -tcsh
root	11643	0.00	0.00	0	0	?	Sep06	1:31 [kworker/15:2H]



The screenshot shows the output of the 'top' command in a terminal window. It displays system statistics, including tasks, memory usage, and a list of running processes with their PID, USER, PR, NI, VIRT, RES, SHR, S, CPU, MEM, TIME+, and COMMAND.

PID	USER	PR	NI	VIRT	RES	SHR	S	CPU	MEM	TIME+	COMMAND
10037	sjames5	20	0	164236	2468	1524	1	0.7	0.0	0:00.15	top
3058	anarghya	20	0	2093048	51240	16120	5	0.3	0.2	0:05.08	node
1	root	20	0	0	0	0	S	0.0	0.0	20:11.37	systemd
2	root	20	0	0	0	0	S	0.0	0.0	0:02.54	kthreadd
3	root	20	0	0	0	0	S	0.0	0.0	0:02.43	ksofirqd/0
5	root	0	-20	0	0	0	S	0.0	0.0	0:00.00	kworker/0:+
6	root	20	0	0	0	0	S	0.0	0.0	1:09.37	kworker/u6+
8	root	rt	0	0	0	0	S	0.0	0.0	0:00.93	migration/0
9	root	20	0	0	0	0	S	0.0	0.0	0:00.00	rcu_bh
10	root	20	0	0	0	0	S	0.0	0.0	9:21.24	rcu_sched
11	root	0	-20	0	0	0	S	0.0	0.0	0:00.00	lru-add-dr+
12	root	rt	0	0	0	0	S	0.0	0.0	0:30.28	watchdog/0
13	root	rt	0	0	0	0	S	0.0	0.0	0:07.69	watchdog/1
14	root	rt	0	0	0	0	S	0.0	0.0	0:00.45	migration/1
15	root	20	0	0	0	0	S	0.0	0.0	0:00.84	ksofirqd/1
17	root	0	-20	0	0	0	S	0.0	0.0	0:00.00	kworker/1:+
19	root	rt	0	0	0	0	S	0.0	0.0	0:07.20	watchdog/2

Windows
Built-in

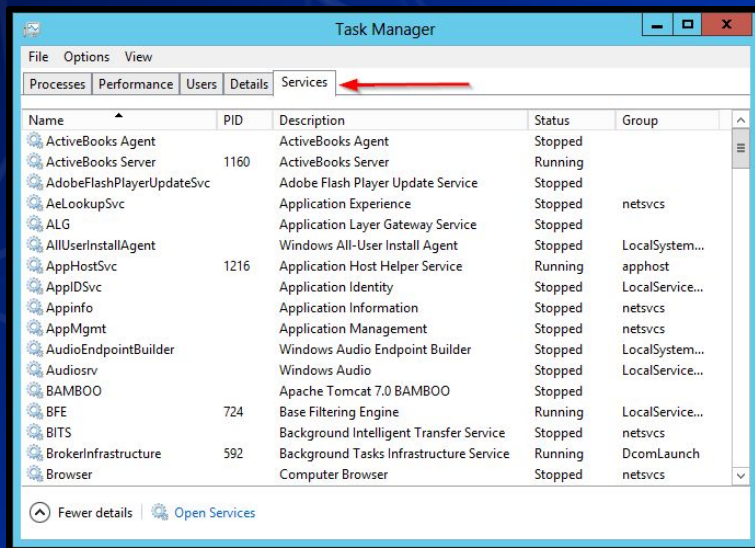
Process
Hacker

\$ps -aux

\$top

How do we see our machine's services?

- Service managers
- How else can we find services?



```
UNIT FILE                                STATE                                VENDOR PRESET
proc-sys-fs-binfmt_misc.automount      static                              enabled
-.mount                                generated                          enabled
boot-efi.mount                          generated                          enabled
dev-hugepages.mount                    static                              enabled
dev-mqueue.mount                       static                              enabled
proc-sys-fs-binfmt_misc.mount           disabled                           enabled
run-vmblock\x2dfuse.mount              enabled                            enabled
snap-core18-2128.mount                 enabled                            enabled
snap-gnome\x2d3\x2d34\x2d1804-72.mount enabled                            enabled
snap-gtk\x2dcommon\x2dthemes-1515.mount enabled                            enabled
snap-snap\x2dstore-547.mount            enabled                            enabled
snap-snapd-12704.mount                 enabled                            enabled
sys-fs-fuse-connections.mount          static                              enabled
sys-kernel-config.mount                static                              enabled
sys-kernel-debug.mount                 static                              enabled
sys-kernel-tracing.mount               static                              enabled
acpid.path                             enabled                            enabled
apport-autoreport.path                 enabled                            enabled
cups.path                              enabled                            enabled
systemd-ask-password-console.path      static                              enabled
systemd-ask-password-plymouth.path     static                              enabled
systemd-ask-password-wall.path         static                              enabled
lines 1-23
```


Sneaky Services

- Network scans can expose ports that are open and closed.
- Open ports show which services may be running
 - ss
 - netstat
- Tools for network reconnaissance (Cyber Kill Chain)
 - **nmap**/zenmap
 - OpenVAS
 - Nikto

In Class Activity

NMAP Activity

NMAP Activity

- ⬡ Use [UbuntuClient](#) to scan [AdminNet](#)
 - ⬡ Install nmap
 - `sudo apt install nmap`
 - ⬡ Read the man pages for nmap
 - `man nmap`
 - ⬡ Use nmap to scan an entire subnet
 - `nmap 10.42.<X>.0/24`
 - ⬡ What did you notice about the results?



NMAP Activity

- Use `OutsideDevice` to scan your `ServerNet`
- `nmap 10.43.<X>.0/24`
- What did you notice about the results?



NMAP Activity

- ⬡ Use `pfctl -d` to disable the firewall
- ⬡ Use `OutsideDevice` to scan `ServerNet`
 - ⬡ `nmap 10.43.<X>.0/24`
 - ⬡ What did you notice about the results?



Logs

- Examples of some logs are:

- File system journals
- Security logs
- System logs
- Application logs

- e.g., `tail -f /var/log/apache2/access.log`

- Why are logs important?

QUESTIONS?

Summary and Wrap-up

Today's achievements:

- Explored the applications of remote and local services
- Initially configured a MySQL database
- Initialized MediaWiki setup
- Utilized application layer network protocols
- Learned how to use network reconnaissance tools