



LINUX SERVICES

LUCAS CRASSIDIS, PHIL FOX

WITH HELP FROM STEPHEN JAMES, AIBEK ZHYLKAI DAROV

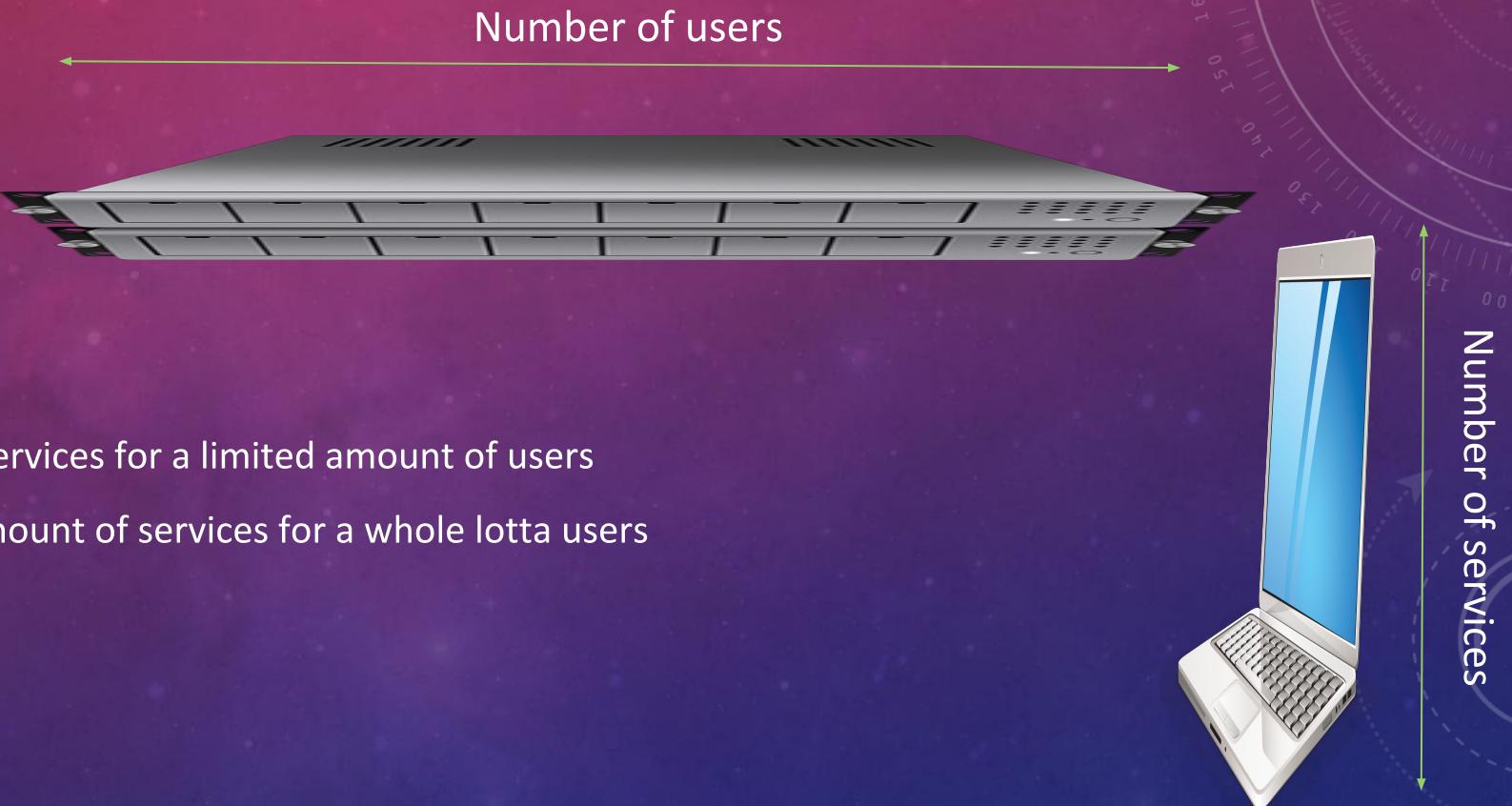
UB NETDEF, SYSTEMS SECURITY

SPRING 2020

AN OVERVIEW:

- It's really awesome that you're here!
 - Today we are introducing some concepts about services
 - We're also walking through an assignment very similar to this week's homework together.
- Take **very good notes** tonight
 - You'll use many similar commands on your homework
 - These slides cover steps. Critical file locations and commands are delivered in-class

YOU GOT SERVED



SERVE THE SERVANTS

- The term "Services" can be ambiguous
 - Technically, your laptop's wireless network manager is a "service."
 - What we're after are server-served services. Which ones can you name?

SERVE THE SERVANTS

- The term "Services" can be ambiguous
 - Technically, your laptop's wireless network manager is a "service."
 - What we're after are server-served services, namely:
 - Website provisioning: Apache: hosting MediaWiki content today, Wiki.js content tomorrow
 - Database storage and retrieval: Maria DB (MySQL) today, PostgreSQL tomorrow

PROTOCOLS

- An agreed-on way to communicate
- What kind of protocols can you name? (Like, real life stuff...)

PROTOCOLS

- An agreed-on way to communicate
- What kind of protocols can you name? (Like, real life stuff...)
- For Machines: Provide a way to store, manage, and access data
- Machines agree on Data types and Ports to transfer data over

PROTOCOL EXAMPLE: DATABASES

- No "standard" ports, DBMSs have their own communication protocols
 - Usually have their own clients to interact with them
- Popular examples:
 - MariaDB/MySQL: 3306/tcp
 - Microsoft SQL Server (MSSQL): 1433/tcp
 - MongoDB: 27017/tcp
 - PostgreSQL: 5432/tcp
 - Redis: 6379/tcp

OTHER SERVICE PROTOCOLS:

- Email: SMTP, POP3, IMAP
- DNS!
- Remote access: RDP (Windows!), SSH
- File transfer: FTP, SCP (SSH)
- Web: HTTP, HTTPS (starting to sound familiar?)
- ...and many more!

IMPLEMENTATION 1: STATIC NETWORKING

- Creds: student, changeme;
- Ubuntu Web Server 192.168.4.[(10*team ID)+1]
 - CLI this time; edits are made to a local file
- Centos DB Server 192.168.4.[(10*team ID)+2]
 - Similar to the web server, but different!
- Linux Client: 192.168.4.[(10*team ID)+3]
 - You've done this before!
- Ping-check when you're done!

IMPLEMENTATION 2: INSTALL SOFTWARE

- Ubuntu Web Server
 - Package manager for Apache services
 - Direct download for Media Wiki HTML/Javascript code, libraries, etc.
- CentOS Database
 - Package manager for all MariaDB/MySQL services

SERVICES TO FOCUS ON: SSH

- This is a remote access protocol that moves a user from one host to another
- Computer Science assignments often require this protocol for turning assignments in!
- Offers secure communication
 - Typically used to access a shell (via the command line) or to remotely execute a command
 - Among other things, it can also be used to copy files (e.g., SCP, SFTP)
- Standard port: 22/tcp
- OpenSSH is, by far, the most common (and free) SSH server

SERVICES TO FOCUS ON: WEB

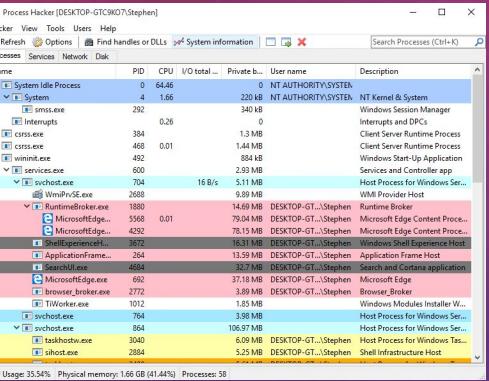
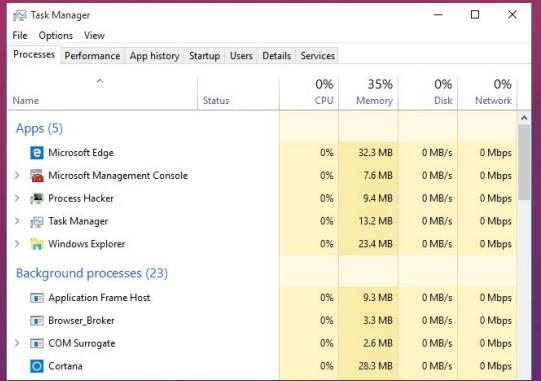
- Web servers process incoming requests from clients for web resources over HTTP and related protocols
 - Web resources are identified by a Uniform Resource Locator (URL)
 - Might perform additional processing while handling the request
- HTTP is unencrypted; data is transmitted in plaintext
 - Anyone on any of the networks on a path from you to the server can see this data
 - VPNs can obscure this otherwise eavesdroppable data
- HTTPS is an extension of HTTP that is encrypted using TLS, or previously, SSL
 - Client is also able to authenticate the server (using the server's certificate often handled by an authority)

SERVICES IN CONCERT: HOW WE GET TO [HTTPS://UBNETDEF.ORG/](https://ubnetdef.org/)

- Get an IP address, gateway, etc.
 - Either via DHCP or static IP configuration (network service)
- Resolve "ubnetdef.org" to an IP address
 - Ask a DNS server for the A (IPv4) records for "ubnetdef.org" (otherwise, AAAA records ref. IPv6)
 - DNS server should respond with "128.205.44.157"
- Send an HTTP GET request to 128.205.44.157 asking for host ubnetdef.org and path "/"
 - TCP handshake starts, and public keys etc. are exchanged (since we're using HTTPS)
 - Client (browsers etc.) will do
 - Web server processes request then responds
- Note that the above steps are simplified: a lot more happens!

HOW CAN I SEE MY MACHINE'S SERVICES?

- Service managers:



- Task Manager
- Process Hacker
- Windows Built-in
- Windows Freeware
- \$ ps
- Linux Built-in
- \$ top
- Linux Built-in

Name	PID	CPU	I/O total ...	Private b... s	User name	Description
System Idle Process	0	64.46	0	NT AUTHORITY\SYSTEM		
System	4	1.66	220 kB	NT AUTHORITY\SYSTEM		NT Kernel & System
smss.exe	292	0.26	340 kB			Windows Session Manager
Interrupts						Interrupt and DPCs
cssseces.exe	384	0.06	1.3 MB			Client Server Runtime Process
cssrss.exe	468	0.01	1.44 MB			Client Server Runtime Process
wininit.exe	492	0.01	884 kB			Windows Start-Up Application
services.exe	600	0.01	2.93 MB			Services and Controller app
ApplicationFrameHost	704	0.01	16 B/s	5.11 MB		Host Process for Windows Services
Wmflauncher.exe	2688	0.01	9.09 MB			Windows Media Host
RuntimeBroker.exe	1880	0.01	14.69 MB	DESKTOP-GT... Stephen		Runtime Broker
MicrosoftEdge	5568	0.01	79.04 MB	DESKTOP-GT... Stephen		Microsoft Edge Content Process
MicrosoftEdge	4292	0.01	78.15 MB	DESKTOP-GT... Stephen		Microsoft Edge Content Process
ShellExperienceHost	3672	0.01	16.31 MB	DESKTOP-GT... Stephen		Windows Shell Experience Host
ApplicationFrameHost	264	0.01	13.59 MB	DESKTOP-GT... Stephen		Application Frame Host
ApplicationFrameHost	4688	0.01	15.53 MB	DESKTOP-GT... Stephen		Application Frame Host
MicrosoftEdge	692	0.01	37.18 MB	DESKTOP-GT... Stephen		Microsoft Edge Content application
Browser_Broker.exe	2772	0.01	3.89 MB	DESKTOP-GT... Stephen		Browser_Broker
TiWorker.exe	1012	0.01	1.85 MB			Windows Modules Installer Worker
svchost.exe	764	0.01	3.98 MB			Host Process for Windows Services
svchost.exe	864	0.01	106.97 MB			Host Process for Windows Services
taskhostw.exe	3040	0.01	6.09 MB	DESKTOP-GT... Stephen		Host Process for Windows Tasks
sihost.exe	2884	0.01	5.25 MB	DESKTOP-GT... Stephen		Shell Infrastructure Host

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+ COMMAND
10057	sjames5	20	0	164236	2468	1624	R	0.7	0.0	0:00.16 top
3058	anarghya	20	0	2093048	51240	16120	S	0.3	0.2	0:05.80 node
1	root	20	0	194816	5952	2724	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 ksoftirqd/0
4	regan	20	0	0	0	0	S	0.0	0.0	0:00.00 kworker/0:+
5	regan	20	0	0	0	0	S	0.0	0.0	0:00.00 kworker/u6:+
6	regan	20	0	0	0	0	S	0.0	0.0	1:09.37 kworker/u6:+
7	regan	20	0	0	0	0	S	0.0	0.0	0:00.93 migration/0
8	root	rt	0	0	0	0	S	0.0	0.0	0:00.00 rcu_bh
9	root	20	0	0	0	0	S	0.0	0.0	0:00.00 rrd_sched
10	root	20	0	0	0	0	S	0.0	0.0	9:21.24 rrd_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 ksoftirqd/1
16	root	20	0	0	0	0	S	0.0	0.0	0:00.00 kworker/1:+
17	root	0	-20	0	0	0	S	0.0	0.0	0:00.00 kworker/1:+
18	root	0	0	0	0	0	S	0.0	0.0	0:07.20 watchdog/2

```
top - 18:19:56 up 32 days, 18:07, 6 users, load average: 0.00, 0.01, 0.05
Tasks: 275 total, 1 running, 272 sleeping, 2 stopped, 0 zombie
%Cpu(s): 0.0 us, 0.0 sy, 0.0 ni, 99.9 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
KiB Mem : 32932400 total, 26738652 free, 456824 used, 5736924 buff/cache
KiB Swap : 32767996 total, 31865596 free, 902400 used. 31371832 avail Mem

PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
10057 sjames5 20 0 164236 2468 1624 R 0.7 0.0 0:00.16 top
3058 anarghya 20 0 2093048 51240 16120 S 0.3 0.2 0:05.80 node
1 root 20 0 194816 5952 2724 S 0.0 0.0 20:11.37 systemd
2 root 20 0 0 0 0 0 S 0.0 0.0 0:02.54 kthreadd
3 root 20 0 0 0 0 0 S 0.0 0.0 0:02.43 ksoftirqd/0
4 regan 20 0 0 0 0 0 S 0.0 0.0 0:00.00 kworker/0:+
5 regan 20 0 0 0 0 0 S 0.0 0.0 0:00.00 kworker/u6:+
6 regan 20 0 0 0 0 0 S 0.0 0.0 1:09.37 kworker/u6:+
7 regan 20 0 0 0 0 0 S 0.0 0.0 0:00.93 migration/0
8 root rt 0 0 0 0 0 S 0.0 0.0 0:00.00 rcu_bh
9 root 20 0 0 0 0 0 S 0.0 0.0 0:00.00 rrd_sched
10 root 20 0 0 0 0 0 S 0.0 0.0 9:21.24 rrd_sched
11 root 0 -20 0 0 0 0 S 0.0 0.0 0:00.00 lru-add-dr+
12 root rt 0 0 0 0 0 S 0.0 0.0 0:30.28 watchdog/0
13 root rt 0 0 0 0 0 S 0.0 0.0 0:07.69 watchdog/1
14 root rt 0 0 0 0 0 S 0.0 0.0 0:00.45 migration/1
15 root 20 0 0 0 0 0 S 0.0 0.0 0:00.84 ksoftirqd/1
16 root 20 0 0 0 0 0 S 0.0 0.0 0:00.00 kworker/1:+
17 root 0 -20 0 0 0 0 S 0.0 0.0 0:00.00 kworker/1:+
18 root 0 0 0 0 0 0 S 0.0 0.0 0:07.20 watchdog/2
```

FINDING HARDER TO SEE SERVICES:

- Scan your network/hosts
 - Red and Blue team tactic
- Network/host scans can expose ports that are open/closed/filtered
- Open ports show which services might be running
 - Tools like `nmap` provide further detail on which specific services (including versions) are installed

DEEPEST SERVICES DIVE:

- Further means exist to show exactly which services are running when!
- Configuration files
 - Databases, remote access, web, file transfer
- Logs
 - All of the above AND
 - File system journals, security logs, system logs, etc.

IMPLEMENTATION 3: CONNECT

- CentOS Database first:
 - Add a unique database user that the Web Server (will expect) to see
 - This helps with security!
- Ubuntu Web Server next:
 - Point a client browser at the file system directory
 - Follow the setup instructions; make sure to reference the DB info
 - Download the config file to the client; send (SCP service!) it back to the web server

YOUR HOMEWORK

- Tonight's VMs will be removed – You will rebuild on vCenter
- Uses the same “hardware” and operating systems
- Expects different web code/scripts (Wiki.js) and database protocol (PostgreSQL)
- Is generally a little easier to implement. Nice.
 - Hint: PostgreSQL uses different \s \y \s \t \e \m commands, but use the same QUERELY language as MariaDB;

WHAT QUESTIONS DO YOU HAVE?

- DISCLAIMER We may or may not be available to help on Mattermost Sunday evening, or at all that day
 - Plan wisely, work early
 - Uncontroversial: This is one of the top 3 most difficult assignments



4GIFS.com

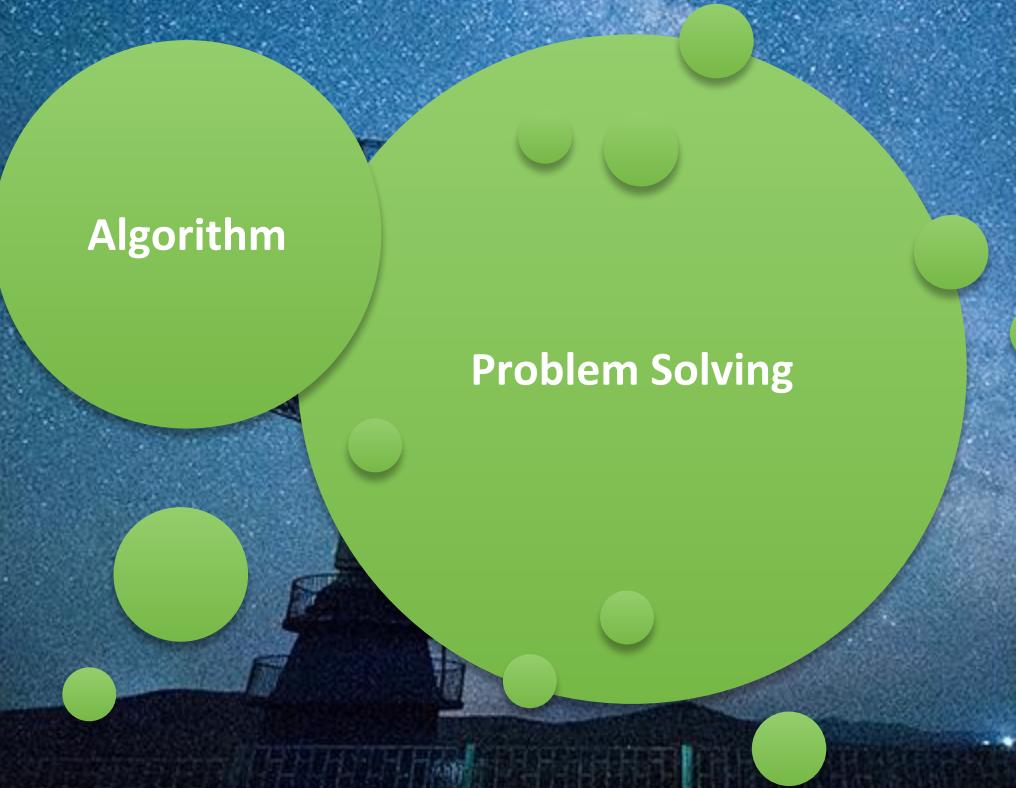
ROCK 'N' ROLL

@XPHILFOX



ASSERT DOMINANCE

@WILDCARD



Algorithm

Problem Solving

Automation