LINUX SERVICES

LUCAS CRASSIDIS, PHIL FOX

WITH HELP FROM STEPHEN JAMES, AIBEK ZHYLKAIDAROV

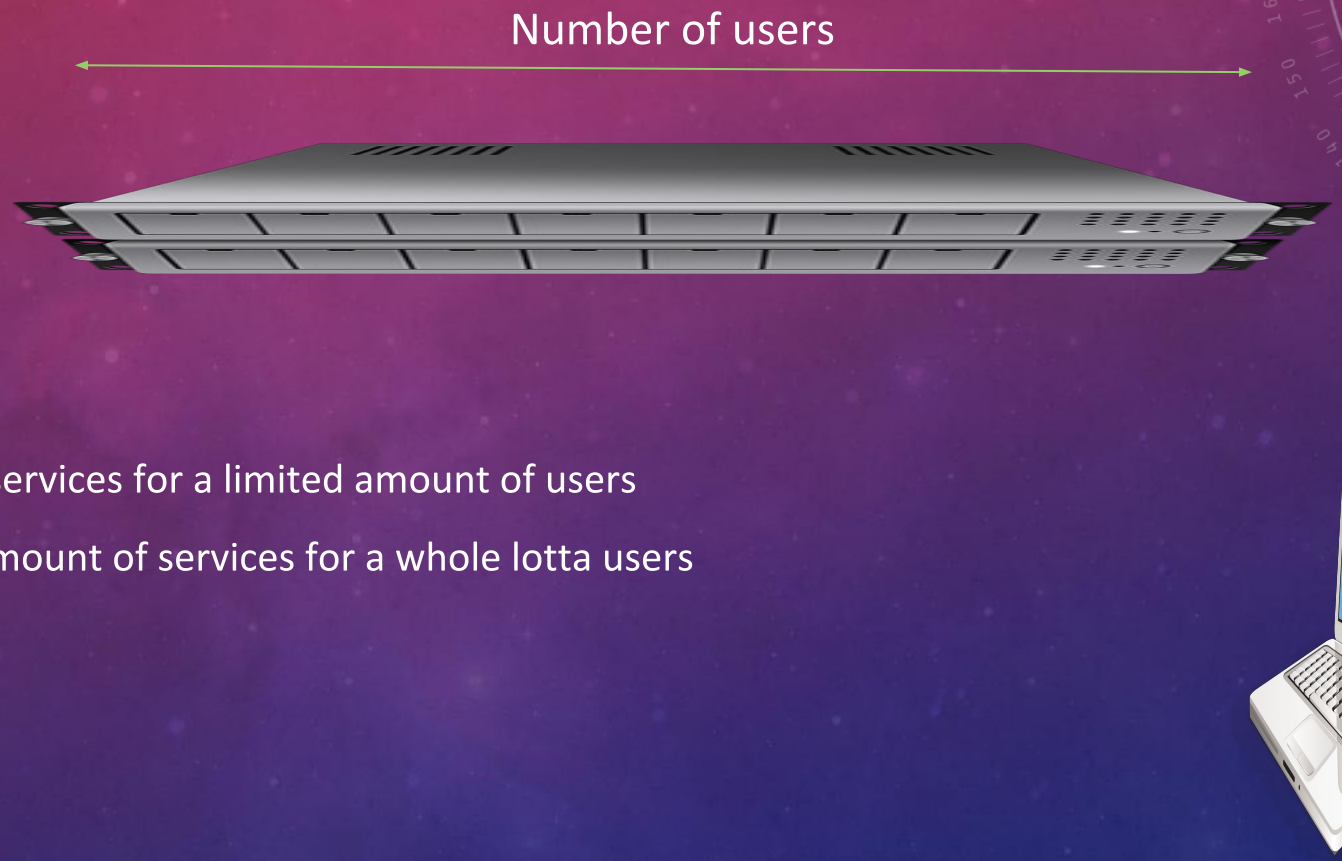
UB NETDEF, SYSTEMS SECURITY

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



- In GENERAL:
  - A client: Runs a bunch of services for a limited amount of users
  - A server: Runs a limited amount of services for a whole lotta users

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

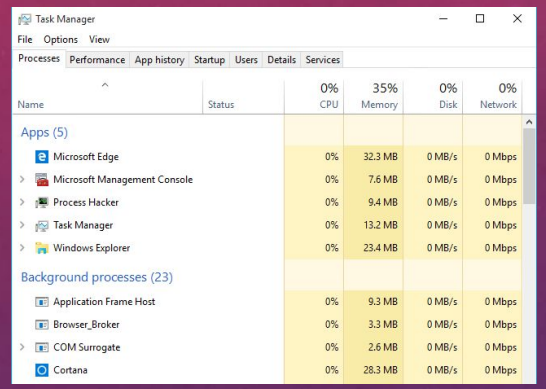
- Web servers process incoming requests from clients for web resources over HTTP and related protocols
  - Web resources are identified by a Uniform Resource Locator (URL)
  - Might perform additional processing while handling the request
- HTTP is unencrypted; data is transmitted in plaintext
  - Anyone on any of the networks on a path from you to the server can see this data
  - VPNs can obscure this otherwise eavsdroppable 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)

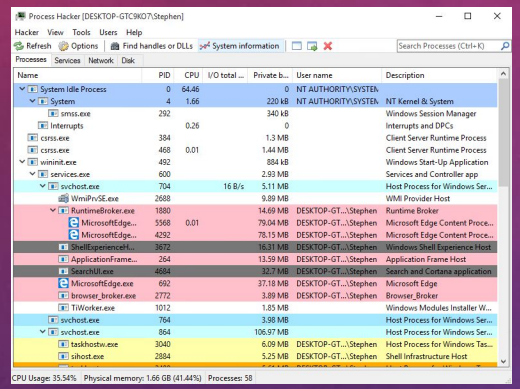
SERVICES IN CONCERT: HOW WE GET TO HTTPS://UBNETDEF.ORG/

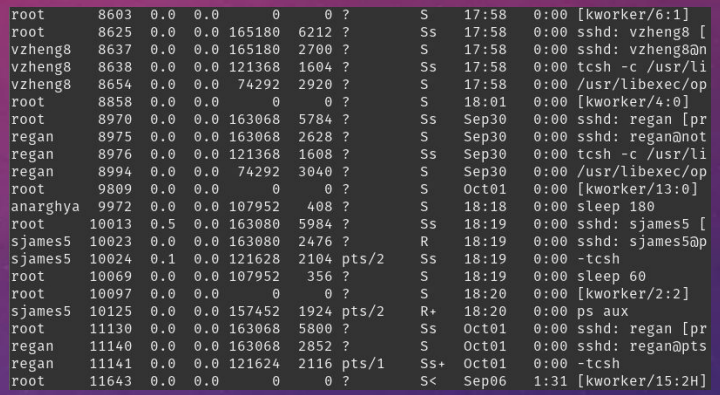
- Get an IP address, gateway, etc.
  - Either via DHCP or static IP configuration (network service)
- Resolve "ubnetdef.org" to an IP address
  - Ask a DNS server for the A (IPv4) records for "ubnetdef.org" (otherwise, AAAA records ref. IPv6)
  - DNS server should respond with "128.205.44.157"
- Send 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!

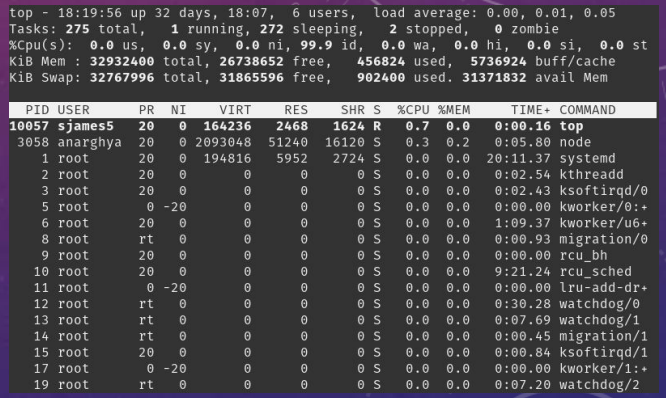
HOW CAN I SEE MY MACHINE'S SERVICES?

- Service managers:









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

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

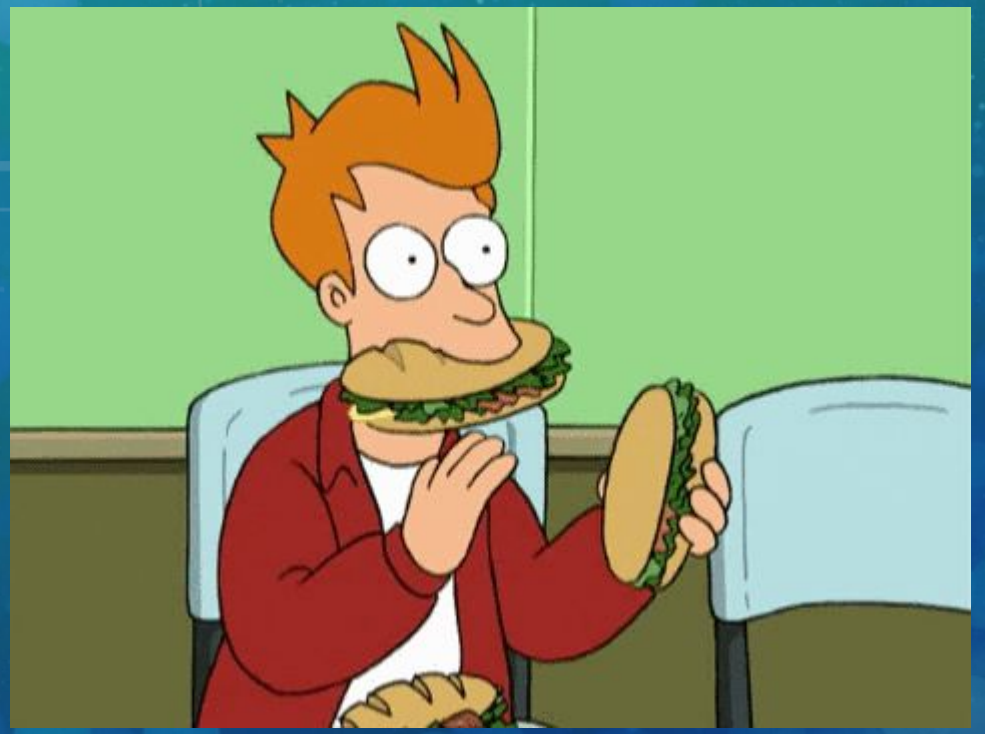
- Tonight's VMs will be removed – You will rebuild on vCenter
- Uses the same “hardware” and operating systems
- Expects different web code/scripts (Wiki.js) and database protocol (PostgreSQL)
- Is generally a little easier to implement. Nice.
  - Hint: PostgreSQL uses different \s \y \s \t \e \m commands,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

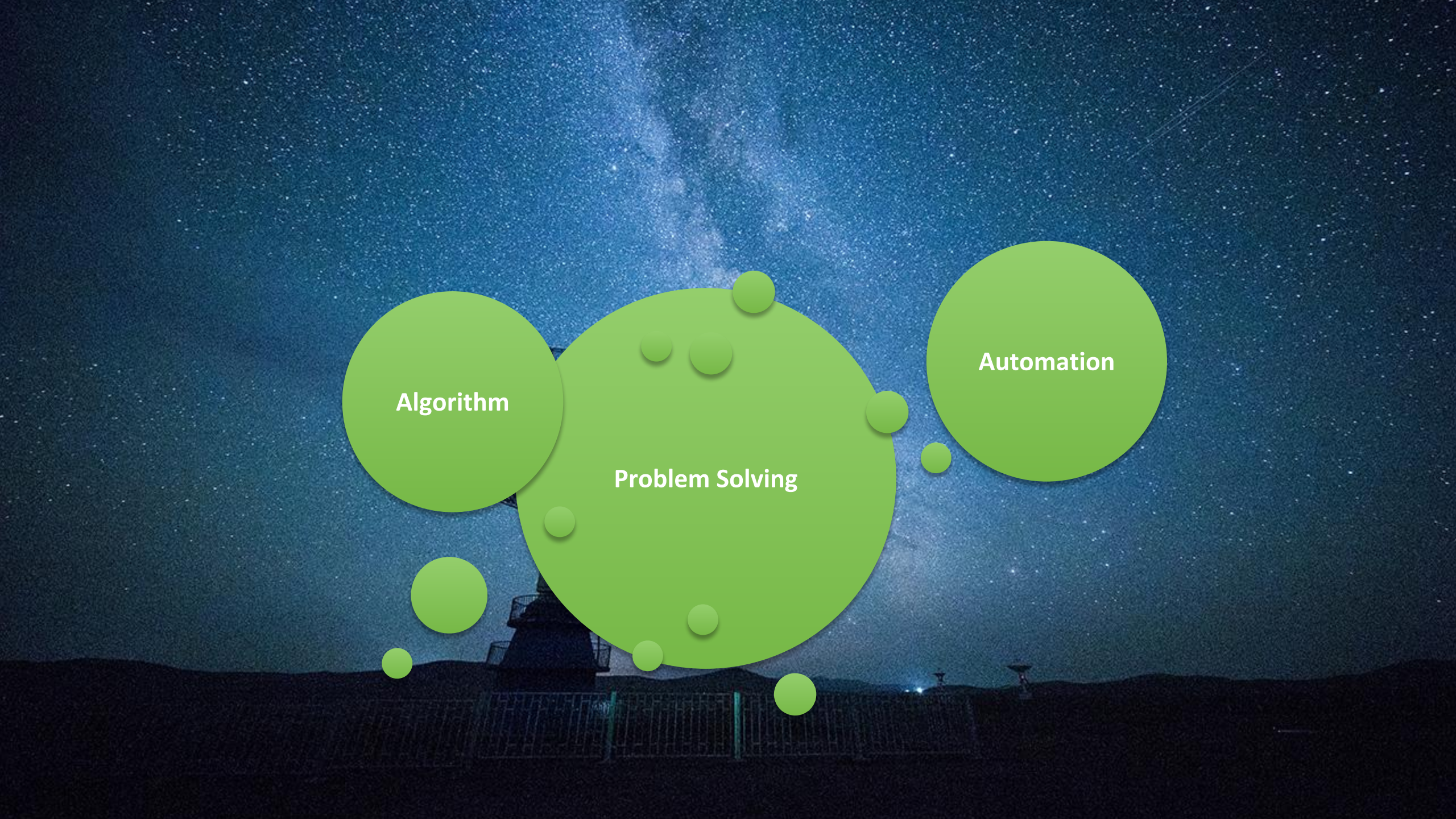
ROCK ‘N’ ROLL

@XPHILFOX



ASSERT DOMINANCE

@WILDCARD


Algorithm
Problem Solving
Automation