

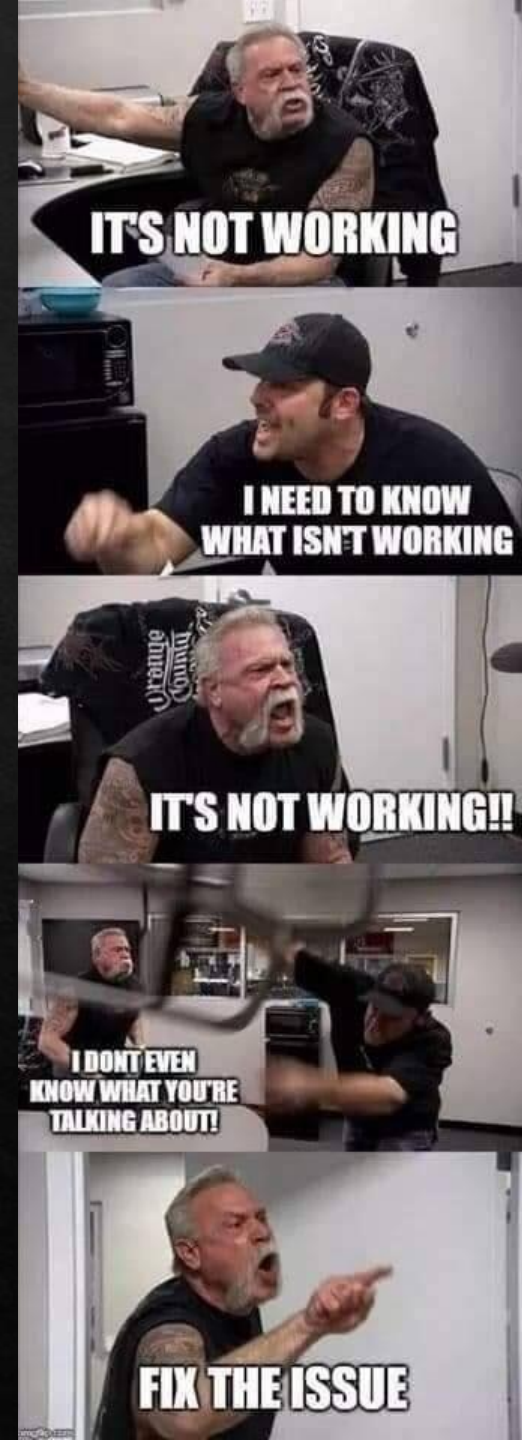
The Metasploit logo is a blue hexagon with a stylized 'M' inside, composed of several rectangular blocks. It is centered in the background of the slide.

# Bug Reporting & Metasploit V2

By Jack Orcherton

# Bug Reporting

- ❖ Unfortunately due to Covid, for us and lecturers it has been a lot harder to debug code remotely, when people give us reports with the words it doesn't work it does not provide us a lot to go on - so please use the 5 W's & H
- ❖ 'It doesn't work' is not useful!



# Who?

- ◆ Who made the code and ensure you are contacting the creator/best person to ask?
- ◆ What is the best way to contact them?



# What?

- ◆ What is the code - e.g the demo script 1 for week 2 in module 123CT fails to work. If it is your own code state the task you are trying to complete and part you are stuck on. Also what is the code meant to do?

# Where?

- ◆ Where are you running the code? Arch, Kali, Parrot, Windows, etc.
- ◆ The program you are using to run the code e.g. Python 3.8

# When?

- ◆ When does the error occur? E.g. is it as soon as you run the code or after you type an input?
- ◆ Does it only happen when you type a particular input?



# Why?

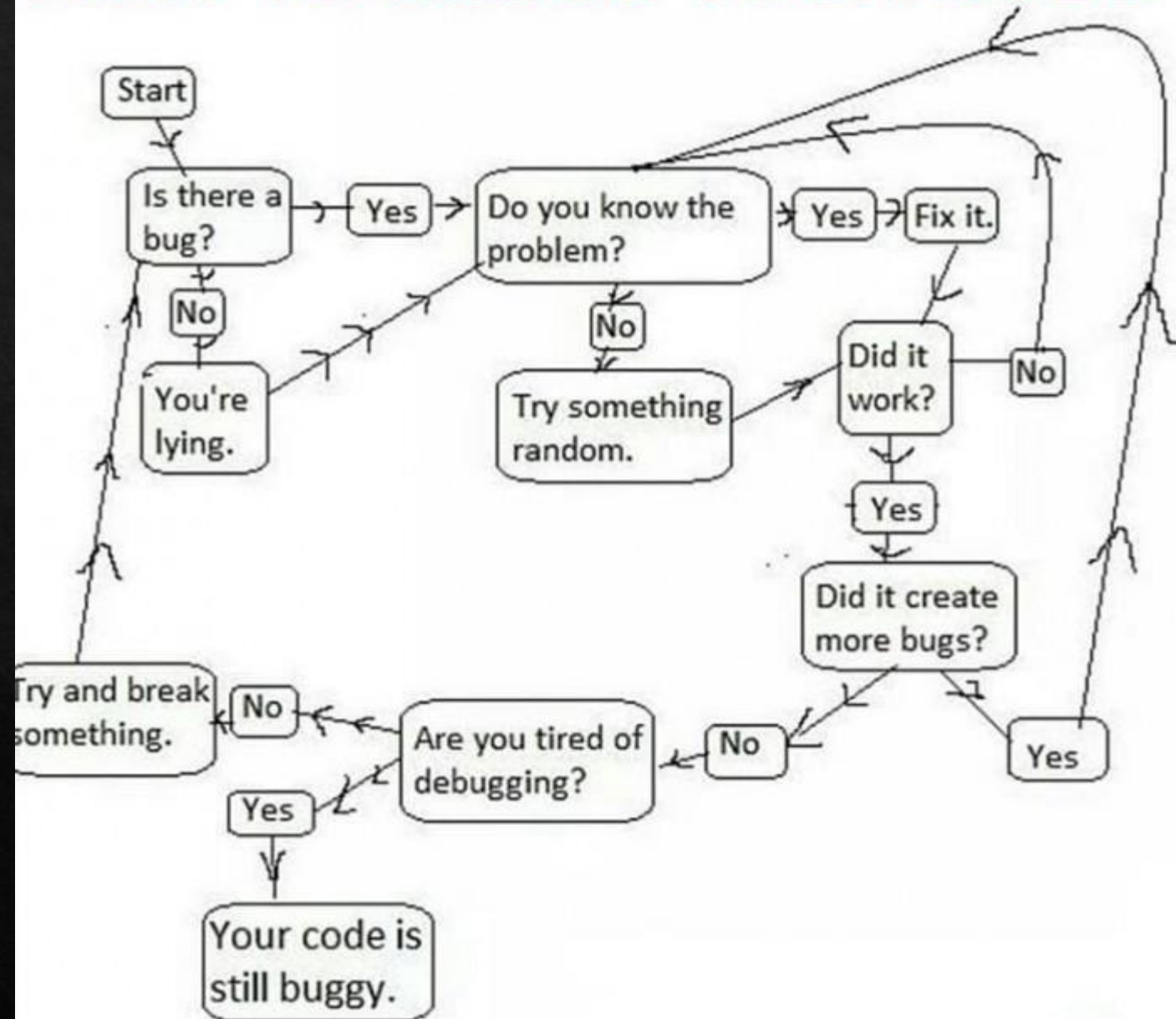
- ◆ Why does the error occur? What is the exact error code/message? (Screenshots of the effected code and error message are helpful.
- ◆ Also make sure that you have read the error code and tried to follow the advice/Duck it/RTFM.
- ◆ Additionally it is helpful that you send a copy of the code in a text, py, etc. file so we can see if we can replicate the error.

# How?

- ◆ How have you attempted to fix the problem? - This shows that you have attempted to fix the issue yourself (try our top 5 mistakes)



# HOW TO DEBUG YOUR CODE



# Top 5 Ethical Hacking Mistakes (trust us we've made many)

- ◆ Spelling - unfortunately I'm bad at this one (the amounts of times I've looked and spelt colour the British way)... common signs are errors like undeclared/unknown variables and unknown commands
- ◆ Permission - very common on Kali that you need to run commands as admin, so just stick 'sudo' in front of the command. Common errors - permission denied.
- ◆ Networking VM's - can't access the internet? Ensuring that VM networking is set to 'NAT'. Using two VM's and can't get them to connect? Ensure they both are on the same network adapter (recommend either host only or NAT)
- ◆ Python Version - unfortunately python 3 is unable to run most python 2 programs, so if one can't run it try the other - best way to tell the difference? Python 2 `print "hi"` Python 3 `print("hi")`
- ◆ Python can't find module - look at installing said module (see pip)

The logo is a blue isometric cube with a black outline. The text "Metasploit V2" is centered within the cube in a white serif font.

Metasploit V2



# Quick Recap

- ◆ Last time:
  - ◆ How to run Nmap scans from within Metasploit (what was the command?)
  - ◆ Metasploit modules (can you name all six?)
  - ◆ Searching for exploits
  - ◆ Selecting exploits
  - ◆ Setting variables (both local & global)
  - ◆ Exploited FTP on Metasploitable VM

# Meterpreter

- ◆ Short Answer – an interactive shell that is made for hackers
- ◆ The shell that we gained access to last session

# It's a Shell

- ◆ This means that your typical linux commands will work to navigate the system (even if it's Windows based)
  - ◆ Cat
  - ◆ Cd
  - ◆ Pwd
  - ◆ Ps
  - ◆ ls



# Plus Added Extra's

- ◆ UPLOAD
- ◆ DOWNLOAD
- ◆ SEARCH
- ◆ GETUID
- ◆ SHELL
- ◆ GETSYSTEM (auto tries to get you admin)
- ◆ Hashdump – print hashed credentials

# And even more

- ◊ Clearev
- ◊ Sysinfo
- ◊ Idletime
- ◊ Migrate
- ◊ Webcam\_snap

