Offensive Golang

Agenda

- What is Go?
- Why does Go appeal to offensive tool developers?
- Getting started with Go
- Basics of Go syntax and features
- Writing our own offensive tooling in Go

What is Go?

- Go (AKA Golang) is a garbage-collected compiled programming language developed by Google
- Go was originally intended for use in “microservices”, that is, highly scalable services for use in enterprise environments
  - The use of microservices is supposed to make projects easier to maintain and easier to scale (many small black boxes rather than one big black box)
- Go has a *huge* standard library (this can be a bad thing!), most of which is implemented in Go, and is designed to make parallel processing as easy as possible through the use of goroutines
  - We’ll talk more about goroutines in a later slide

Why do the bad guys like Go?

- Very easy to write powerful code
  - If tools get discovered and signatured, attackers haven't actually burned that many man hours developing them
- Very easy to cross compile
  - Higher portability -> more targets
  - Support for multiple processor architectures/operating systems (meaning these binaries can run pretty much anywhere)
- *Might* be more difficult to reverse engineer
  - This might just be because a lot of RE tools are/were still catching up on actually analyzing Go binaries
- Compiles to a binary file (PE/ELF)
  - No need to have an interpreter on the target, requires decompilation for static analysis
- Many useful libraries developed by third parties

Alright, I love it, how do I get it?

- You can develop in Go on pretty much any system, but I'll be covering the installation in Ubuntu with VSCODE as our development environment

- Time for a live demo!

Wait, what just happened?

- Install Ubuntu 20.04
  - Bare metal or virtualized
    - I really recommend virtualizing your development machine + taking snapshots every so often, never know when it’s going to save your ass
- Use Snap to install vscode
  - sudo snap install code --classic
- Update/Upgrade apt, then use apt to install go
  - sudo apt update
  - sudo apt upgrade
  - sudo apt install go

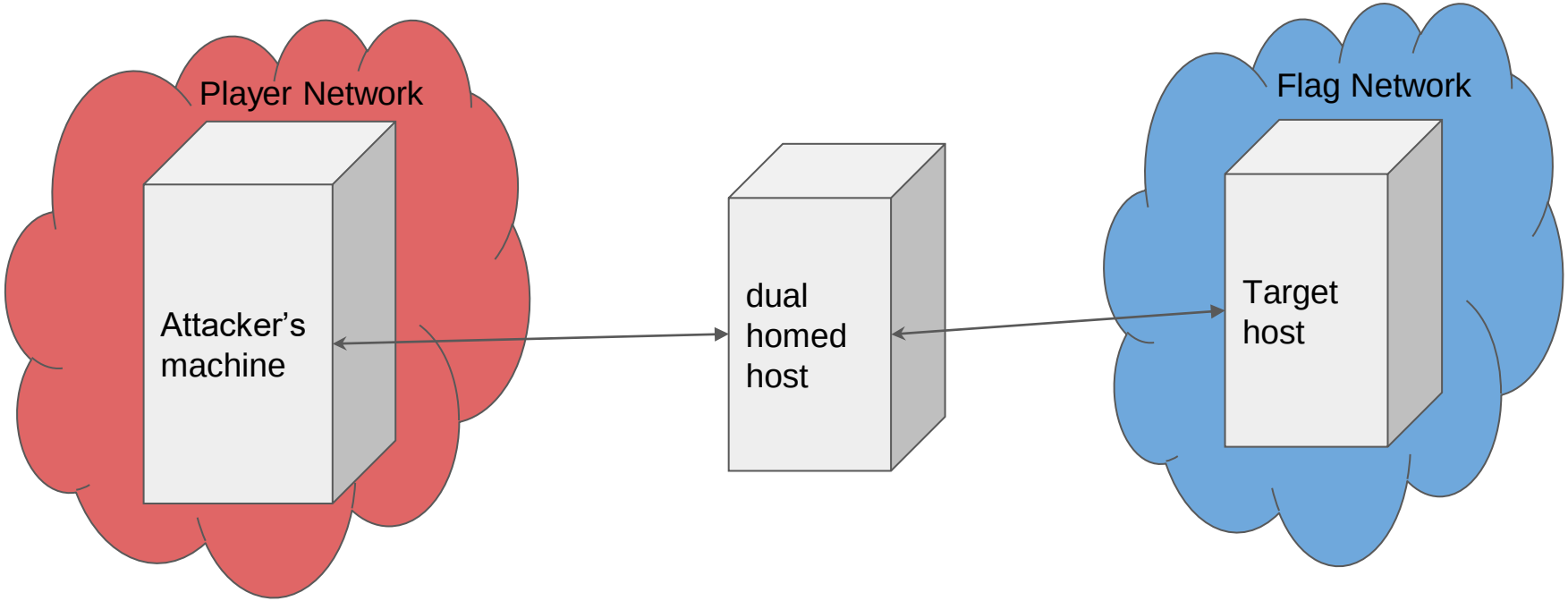
Using Go, with examples

- These examples will introduce you to the syntax of Go

- The examples will be available with these slides after the talk

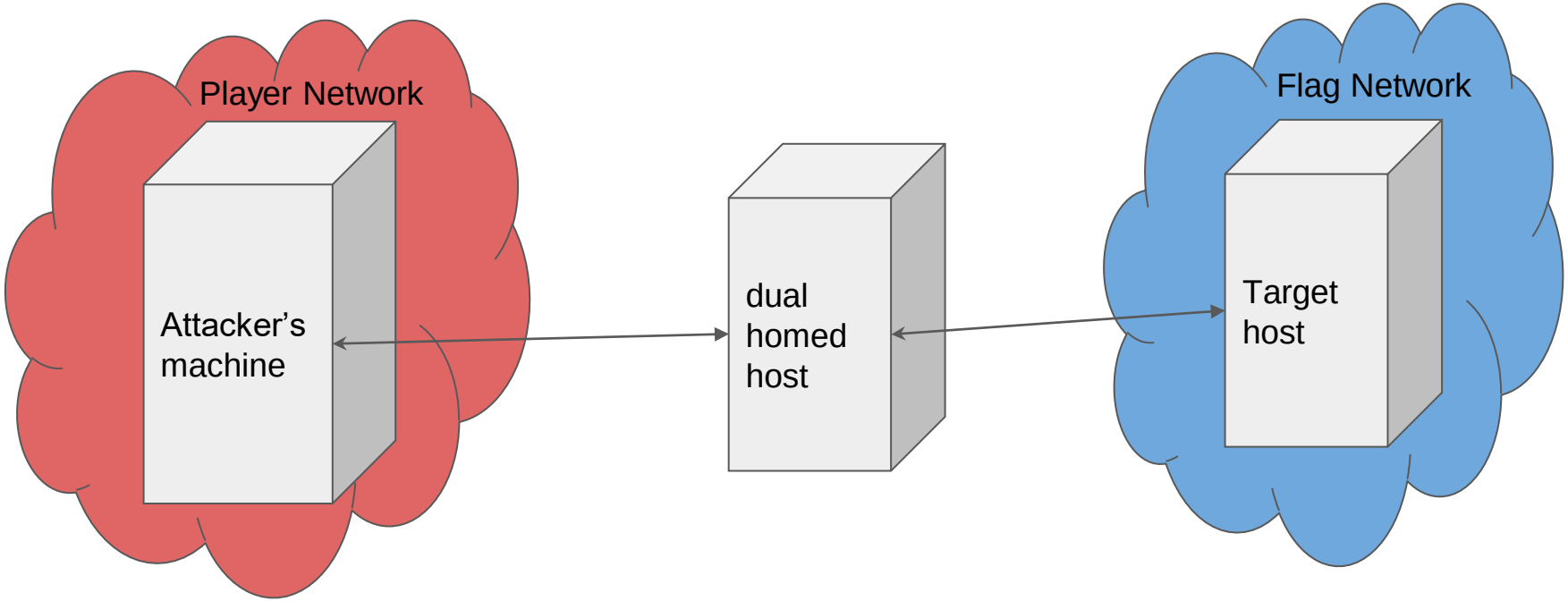
A cool tool!

- Sometimes when doing a CTF or a lab, you'll have to move between parts of the network that are separated by, for example, a multihomed host



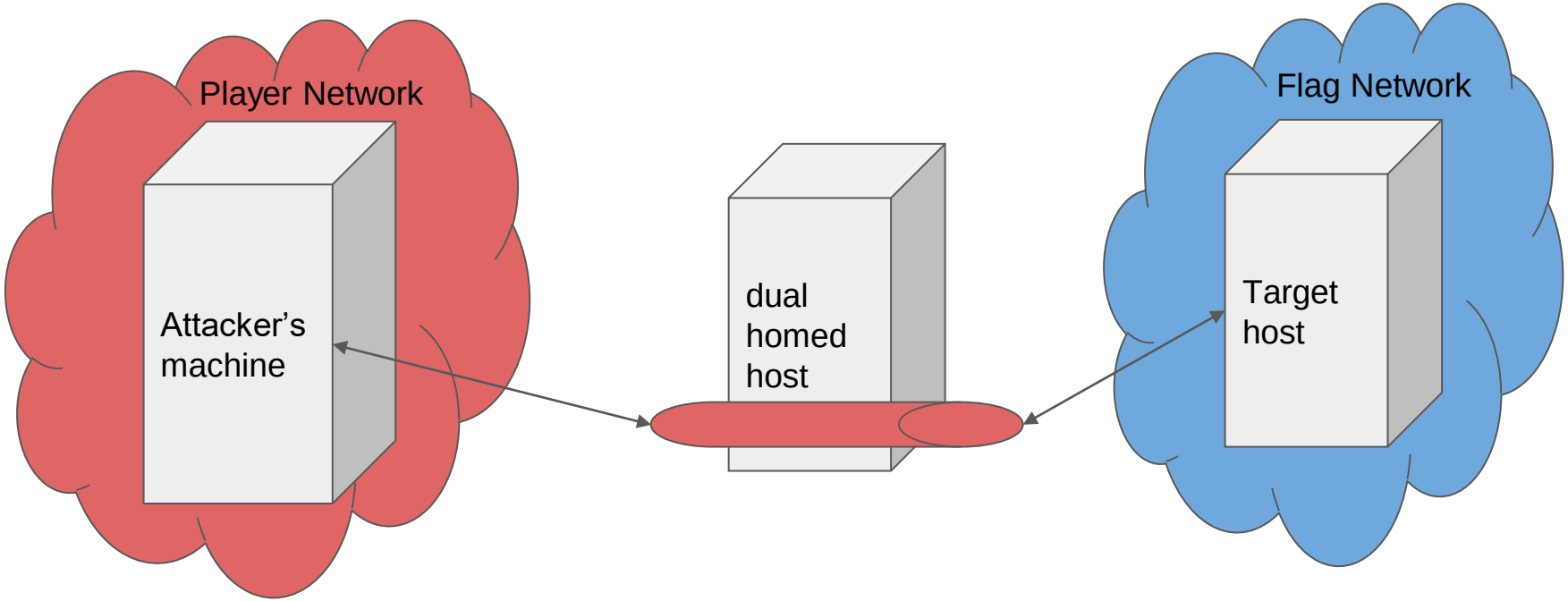
What to do?

- We could move our attack tools onto the dual homed host...



Traffic Proxying

- Or we could create a way to move our network traffic through the dual homed host to the target host



Enter: RevSocks!

- Revsocks is a tool to create a tls-encrypted reverse connection that allows traffic forwarding via a SOCKS5 proxy server
  - TLS Encrypted
  - Reverse connection
  - Traffic forwarding
  - SOCKS5 proxy server

- https://github.com/boba8710/revsocks

Proud Sponsors

CACI

EVER VIGILANT

VOLGENAU SCHOOL

MASON

ENGINEERING