CS 155 Section 9

Project 3 Part 4

Agenda

- Project 3 Part 4
  - Overview of MITM
  - Getting Started and Tips & Tricks
- Office Hours for Project 3 Parts 1-4

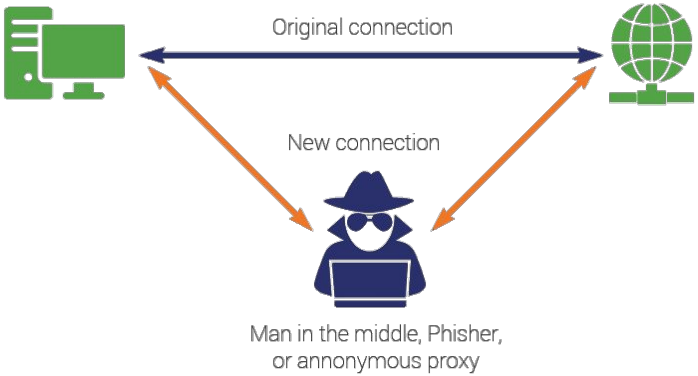
“Onions have layers, ogres have layers.” ~ Shrek

Project 3 Part 4: Monster-in-the-Middle

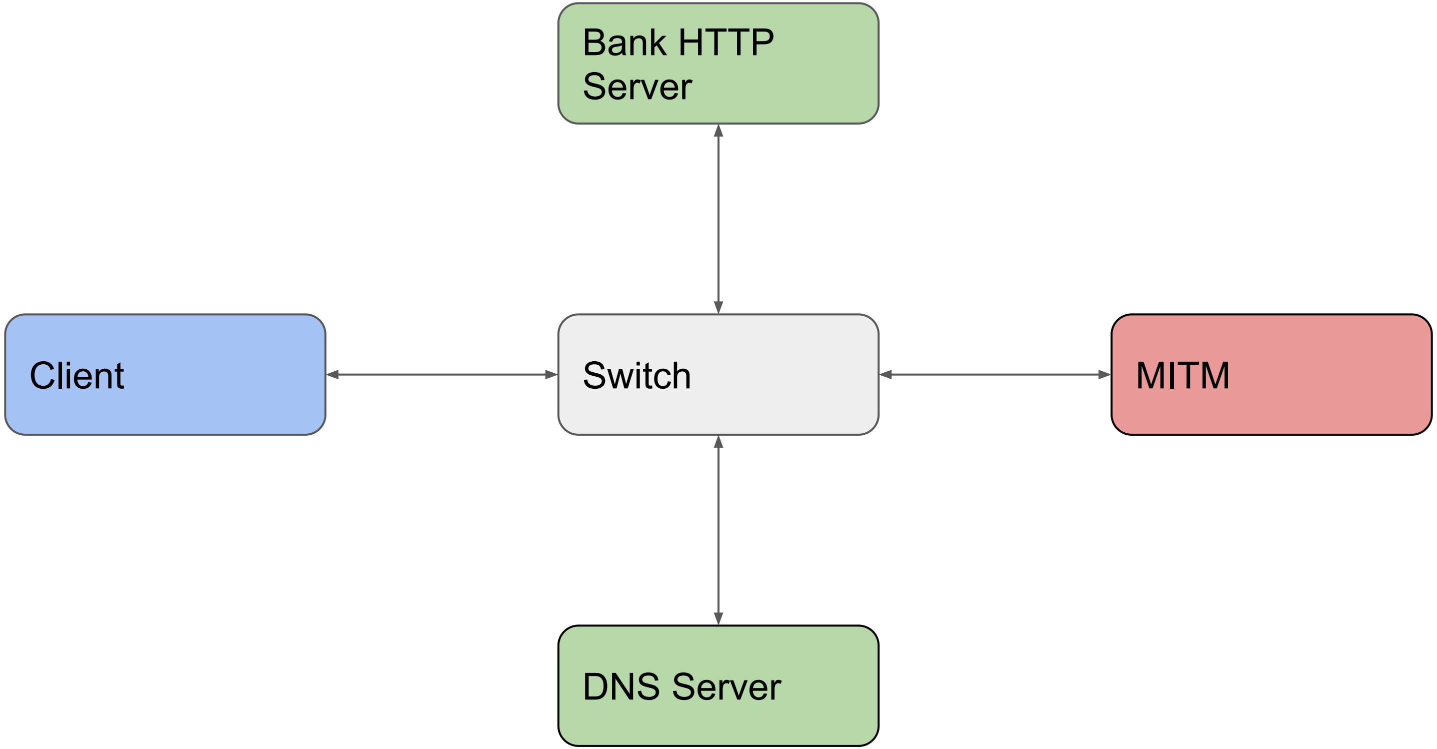
What You Have to Do

Part 4:

- Implement an **MITM** program in Go to hijack HTTP connection

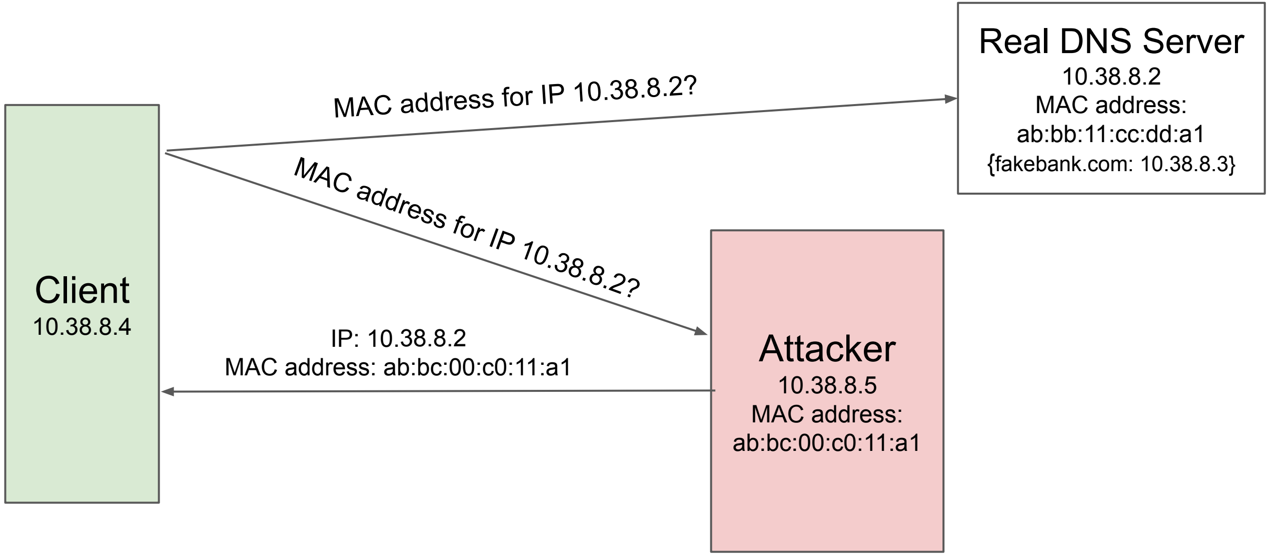


Network Topology Diagram



Monster-in-the-Middle Attack

Spoof ARP response for DNS server MAC address

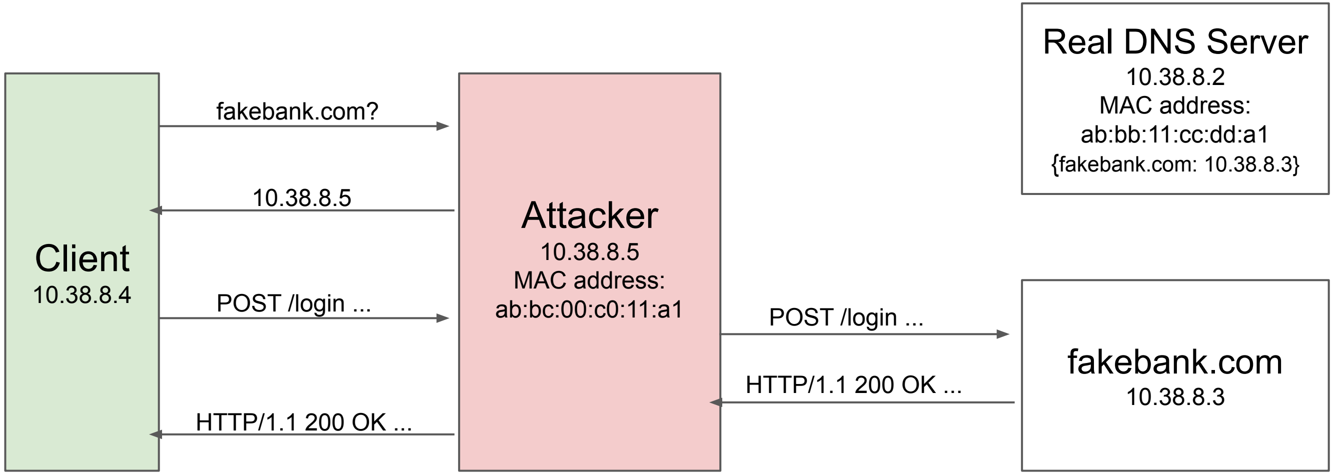


Vulnerabilities:

- Lack of authentication in ARP

Monster-in-the-Middle Attack

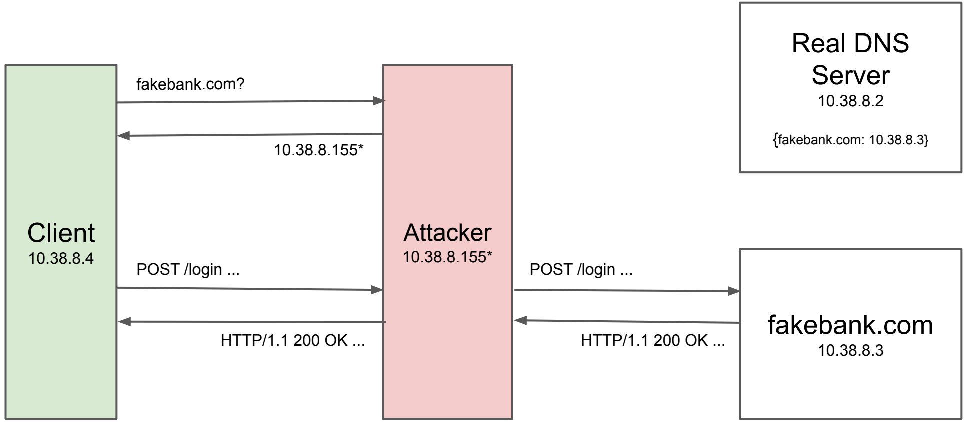
Spoof DNS response for fakebank.com's IP address

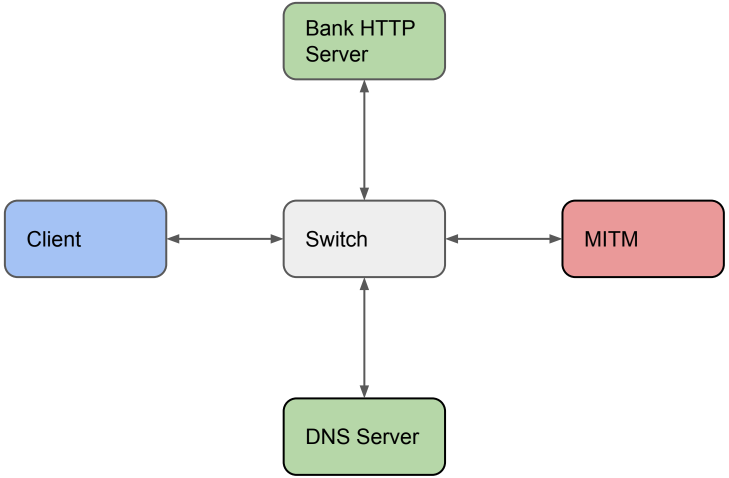


Vulnerabilities:

- Lack of authentication in DNS
- Lack of encryption in plain HTTP

Network Topology Diagram

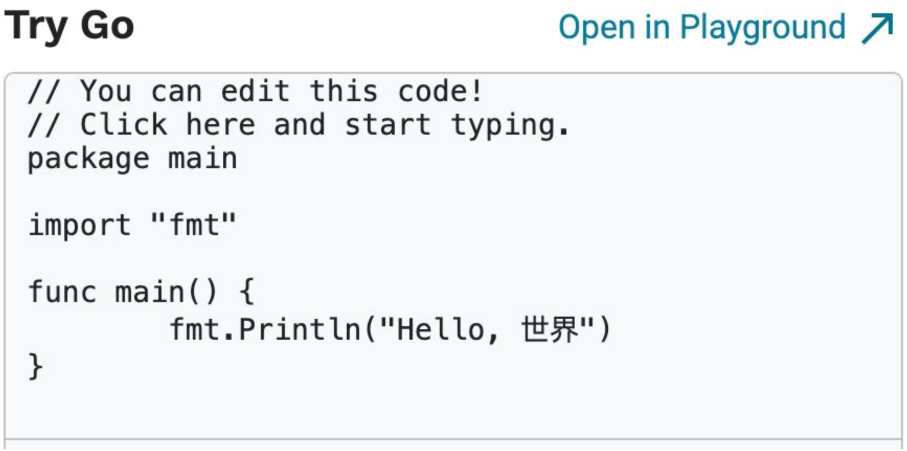




Recap: Learning Go

Download and do the tutorial: A Tour of Go
("Basics" and "Methods and interfaces" sections only)

Use the VSCode Go extension!



Try Go

Open in Playground ↗

```
// You can edit this code!
// Click here and start typing.
package main

import "fmt"

func main() {
	fmt.Println("Hello, 世界")
}
```

Binary distributions available for
Linux, macOS, Windows, and more.

Recap: The gopacket module

https://pkg.go.dev/github.com/google/gopacket

Read the source code for detector.go and mitm.go! Many hints are provided.

Getting Started and Tips & Tricks

Let’s dive into the code!

- Setup
- Testing and debugging
  - Tcpdump + Wireshark
- Overview of the code + file organization
- Other tips and tricks!

Office Hours for Project 3 Parts 1-4