Please open your **CSC436_Environment** Kali VM!!

Scanning with Nmap

Part 2

How would we find…

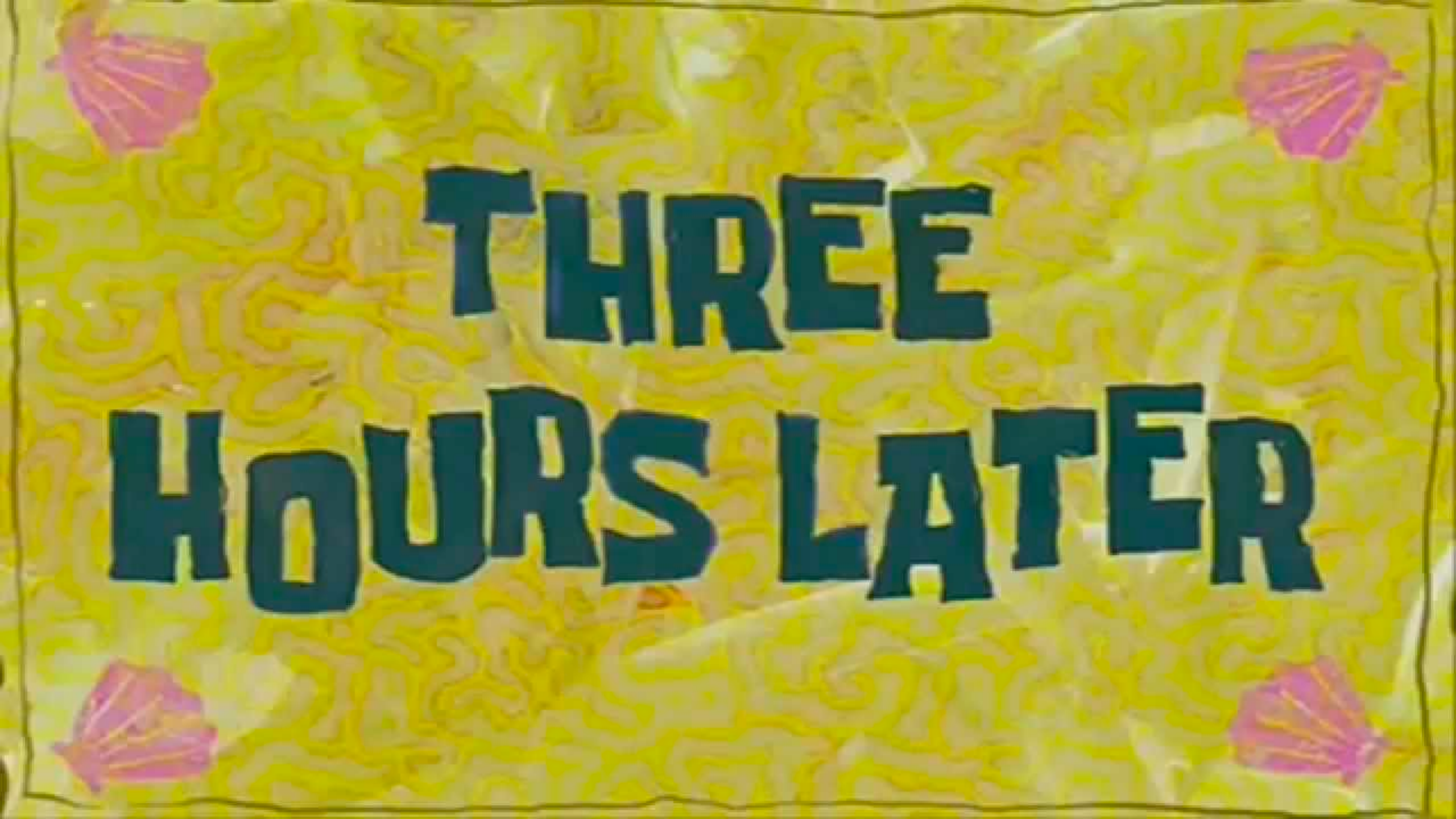
- A webserver running on port 54723?
- How would you know it's a web server and not something else?

- Security by obscurity

Version Scanning!

- …Scan all the things.
- Version Scanning
  - Completes a 3 way handshake and grabs the banner
  - Matches the banner against an internal DB.
  - If no banner, more probing occurs to elicit a response.

```
nmap -sV 10.10.20.53 -Pn -p-
```


THREE
HOURS LATER

This takes a moment

```
nmap -sV 10.10.20.53 -Pn -p-
```

```
Nmap scan report for 10.10.20.53
Host is up (0.00080s latency).
Not shown: 65534 filtered ports
PORT      STATE SERVICE VERSION
43212/tcp open  http    Microsoft IIS httpd 7.5
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https
://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11430.48 seconds
```

Source Port

- Specify which port your scans originate from
- Could increase the likelihood that a scan is allowed in to the network
- Set source port so packets appear normal
- **-g**
- **nmap –sS –g 80 10.10.20.21**

Timing options

- -T0 … Paranoid… 1 packet every 5 minutes
- -T1 … Sneaky … 1 packet every 15 seconds
- -T2 … Polite … 1 packet every .4 seconds
- -T3 … Normal … quickly as possible without missing ports
- -T4 … Aggressive … Wait no more than 1.25 seconds for a response
- -T5 … Insane … waits a maximum of .3 seconds for a response

Output

- **-oA** flag
- Scan results are output in 3 formats
  - .nmap == plaintext
  - .gmnmap == greppable nmap (needed to resume)
    - Use the –resume switch to resume
  - .xml == xml format

Nmap Scripting Engine (NSE)

- Allows scripts to be written to automate networking tasks.
  - Network discovery
  - Vulnerability detection
  - Backdoor detection

NSE

- Can be run as
  - Categories
    - All checks in a category will be run against the target
  - Individual checks
    - Only the specified script will run
- Categories
  - auth, broadcast, brute, default, discovery, dos, exploit, external, fuzzer, intrusive, malware, safe, version, vuln
- Individual
  - Currently 583 scripts
- http://nmap.org/nsedoc

Individual Checks

- Usage:
  - nmap --script <category> <target>
  - nmap --script <script-name> <target>

http-enum

- 10.10.20.58… What ports are open?