ACM NetSec

Cybersecurity Made Simple

Hacking Web Applications
Track

Sign-in form: http://tinyurl.com/y7vp3h5n

ACM NetSec

Web Applications Track Overview

- □ Introduction to web applications
- □ Reconnaissance and Footprinting
- □ SQL Injection
- □ XSS/CSRF
- □ Session Hijacking

Session 1:

Introduction to Web Applications

ACM NetSec

Overview

- ❑ Common Terminologies
- ❑ Common vulnerabilities
- ❑ Web application hacking process
- ❑ Setting up DVWA

Common Terminology

Website

- Displays content
- (Mostly) same information to all visitors
- **E.g. news.ycombinator.com, www.nytimes.com**

Web application

- Interacts with the user and displays content
- Relies on user input and real-time data processing
- **E.g. Facebook messenger**

Web server

Stores and serves resources

Software: **nginx, Apache, IIS**

Client/host model → **HTTP protocol**

HTTP daemon → **Runs in the background and waits for HTTP requests**

IP Addresses

Analogous to your home address or return address on a piece of mail

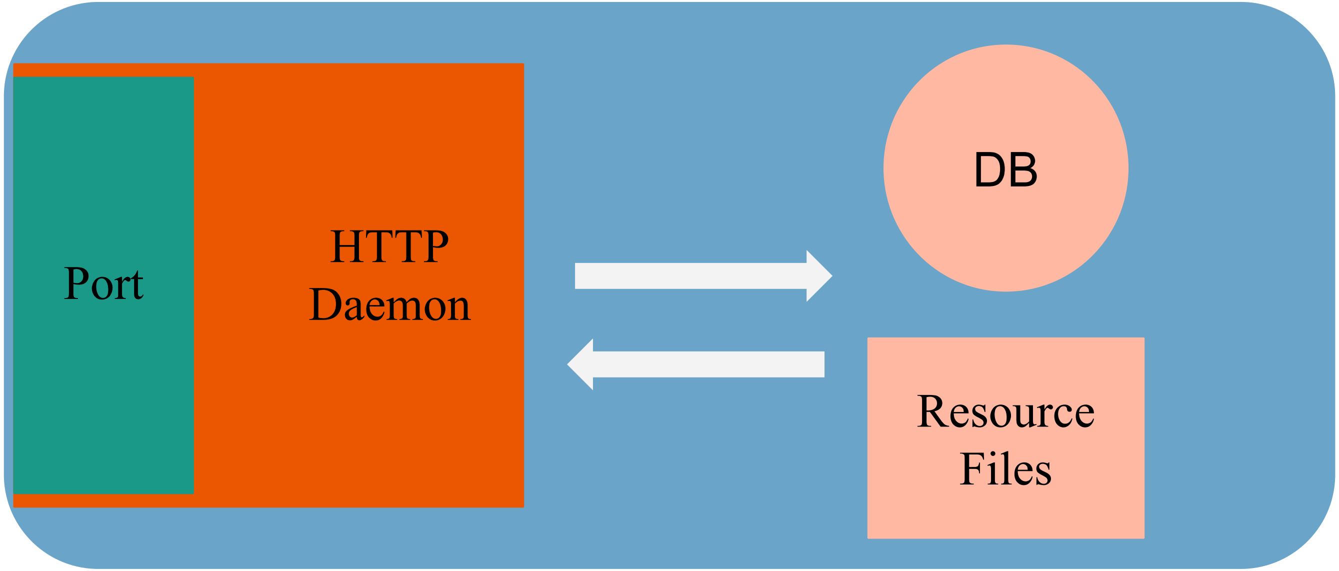
Used to identify computers on the Internet

E.g. 192.168.123.2

Viewing your IP address (you can have more than one!)

- *ipconfig (command line tool on Windows) / ifconfig (on Mac/Linux)*
- *Google "what is my ip"*

Web server



Ports

Analogous to seaports

Each port is assigned **a particular function by the IANA**

Commonly range from 0 to 1023:

- **80 : Http protocol**
- **443: Https protocol**
- **22: SSH**

Client/Host Model

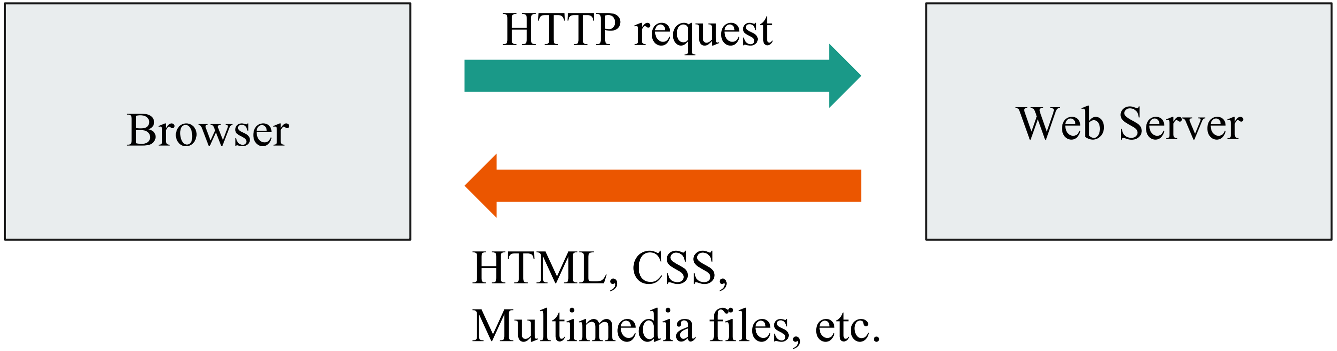
Client is an application that **requests resources** from a web server.

Internet Browser

Host is the server that **provides resources**. Tasked to process any request for resources and return the relevant resources.

Web Server

Client/Host Model



Browser

HTTP request

Web Server

HTML, CSS,
Multimedia files, etc.

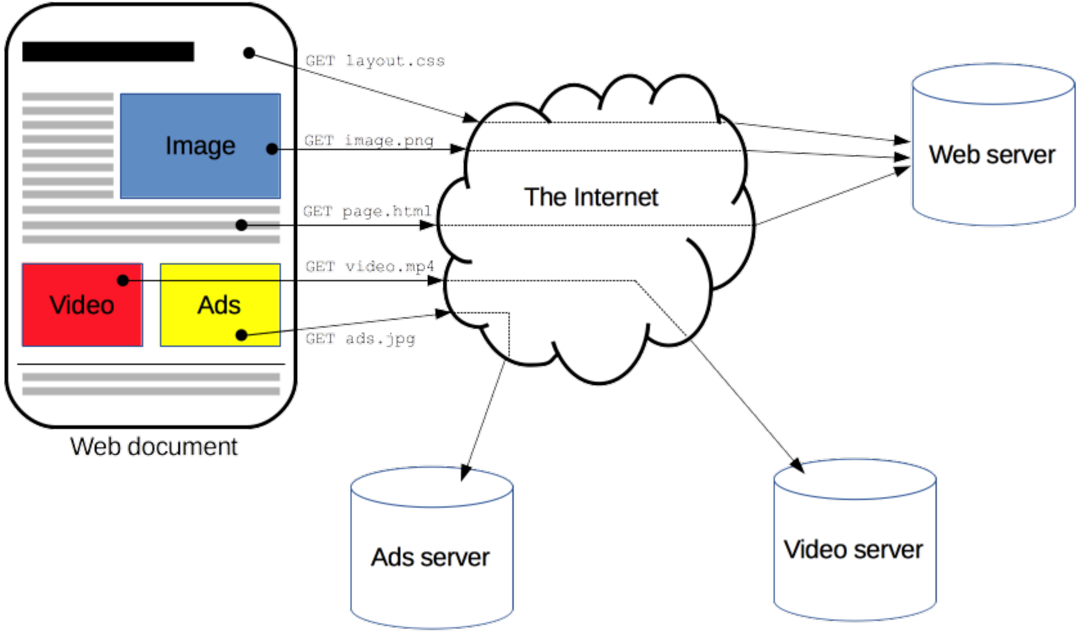
Constructs and **sends** HTTP requests
Translates the resource files

Receives HTTP request

Returns resources associated with the request

Source: https://developer.mozilla.org/en-US/docs/Web/HTTP/Overview

HTTP Protocol



Back-end and Front-end

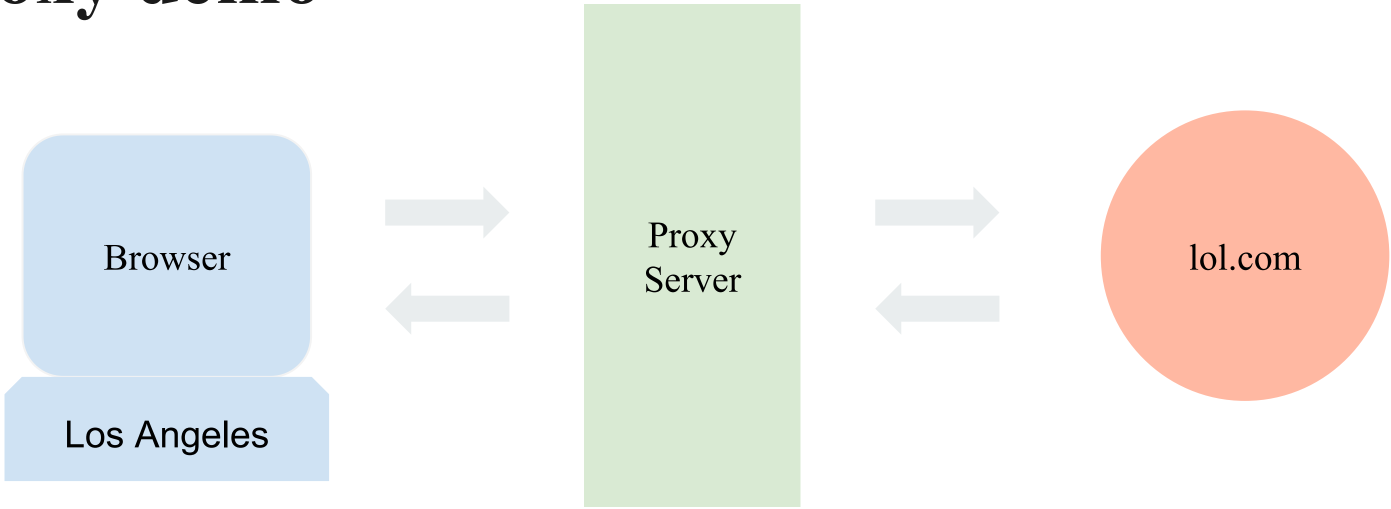
- **Front-end:**
  - What the user **sees and interacts with**
  - UI/UX
  - Styles
- **Back-end:**
  - The “server-side"
  - **Underlying logic and algorithms**
  - **Databases**

Proxy Servers

- **Intermediary endpoint** between device and server

- **Why** a proxy server ?
  - Cache
  - Improve user response time
  - Monitor traffic
  - Anonymity

Proxy demo



IP address points to a location in New York

Application thinks you’re located in New York

Proxy Servers

- But….
- Using (forward) proxy servers is extremely risky:
  - Owner of the server might be able to monitor your internet history.
  - You don’t really have complete anonymity.
- Unless you are using a UCLA proxy server or one operated by someone you trust

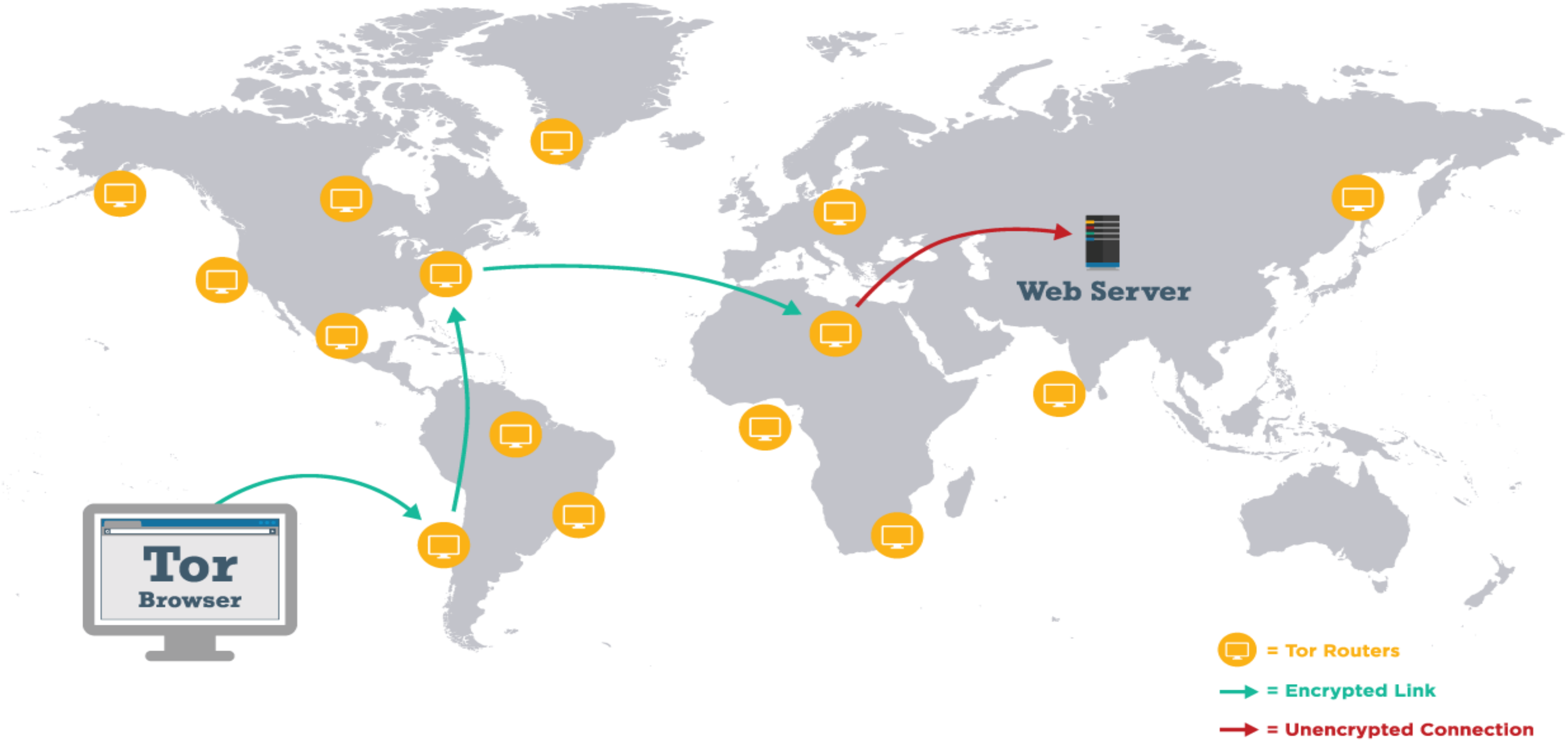
The Darknet

ACM NetSec

Darknet

- What is it?
    - Any network that can be accessed with non-standard communication methods
- ToR = The Onion Router, The Freenet Project, I2P (Invisible Internet Project)
- Can’t the government still see that I use ToR?
- BE CAREFUL!!!

How The Tor Network Works



Wordfence™

wordfence.com/learn

Common Steps In Hacking Web Applications

ACM NetSec

Step 1:
Know your target

ACM NetSec

Why is it important ?

Web server programs and programming languages have unique vulnerabilities

Examples:

- Strcmp in PHP
- SQL Injection in older versions of Drupal
- Exploits in Ruby Gems

How ?

Analyze HTTP header responses

Use web services such as builtwith.com

Social Engineering

Access config files

Use vulnerability scanning tools

Use nmap

Common Vulnerability Scanning Tools

Burp

Netsparker

OWASP Zed

Step 2:
Look up possible exploits

CVE Common Vulnerabilities and Exposures

Security risks for most programming languages and frameworks

https://cve.mitre.org/index.html

Step 3 : Attack

Examples of Simple Exploits

Strcmp function PHP

Directory traversal

Checking .gitignore

Checking robot.txt/ admin files/ db files/ config files

Simple SQL injection

Setting up DVWA (Damn Vulnerable Web App)

1. Download XAMPP
2. Download DVWA from Github
3. Move DVWA directory to /Applications/XAMPP/htdocs
4. Setup config/config.php
5. Go through the README
6. Play around with DVWA

DVWA Demo

ACM NetSec

Next Week: Reconnaissance and Footprinting

Thank you ＼(￣▽￣)/

Feedback form: http://bit.ly/2gO0acZ

ACM NetSec