Sig•Mal

Meeting 6

Advanced Basics Terms

- Cloud → Collection of computers with large storage capabilities that remotely serve requests ~Access to files from all around the world.
- VPN → A tool that allows the user to remain anonymous while using the internet by masking the location and encrypting traffic.
- Exploit → A malicious bit of code that can take advantage of a vulnerability
- Payload → Carries the exploit to take control of that thing
- Virus → A type of malware aimed to corrupt, erase or modify information on a computer before spreading to others.
- Rootkit → Rootkits exist to provide sustained covert access to a machine, so that the machine can be remotely controlled and monitored in a manner that is extremely difficult to detect
- Keylogger → Records keystrokes that were typed

Advanced Basics Terms

- Ransomware → A form of malware that deliberately prevents you from accessing files on your computer - holding your data hostage. It will typically encrypt files and request that a ransom be paid in order to have them decrypted or recovered.
- Trojan Horse → A piece of malware that often allows a hacker to gain remote access to a computer through a “back door”.
- Worm → A piece of malware that can replicate itself in order to spread the infection to other connected computers.
- Bot / Botnet → A type of software application or script that performs tasks on command, allowing an attacker to take complete control remotely of an affected computer. A collection of these infected computers is known as a “botnet” and is controlled by the hacker or “bot-herder”.
- Backdoor → A backdoor is a typically covert method of bypassing normal authentication or encryption in a computer, product, embedded device, or its embodiment

Advanced Basics Terms

- Spyware → A type of malware that functions by spying on user activity without their knowledge. The capabilities include activity monitoring, collecting keystrokes, data harvesting (account information, logins, financial data), and more
- Pen-Testing → Short for “penetration testing,” this practice is a means of evaluating security using hacker tools and techniques with the aim of discovering vulnerabilities and evaluating security flaws.
- DOS → Denial-of-Service ~lol can’t really use this rn
- Social Engineering → A technique used to manipulate and deceive people to gain sensitive and private information ~Being able to talk your way into the password (my favorite tactic)

Advanced Basics Terms

- Clickjacking → A hacking attack that tricks victims into clicking on an unintended link or button, usually disguised as a harmless element.
- Deep fake → Using machine learning to trick so that ppl can be manipulated to do something
- Types of Security People
  - White Hat → Authorized to do something
  - Black Hat → Not authorized to do something but for a malicious purpose
  - Grey Hat → Not authorized to do something but not for a malicious purpose
- Teams
  - Red Team → Attack Team ~simulate a real world attack
  - Blue Team → Defense Team ~make incident response stronger via assessment

CTFs

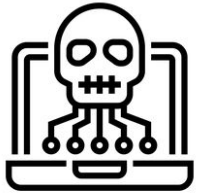
- Capture the Flags
  - ~Like security (cybersecurity) version for Hackathons
    - Instead of Building a project, you will have to “break something down”
- Make you focus on: vulnerability discovery, exploit creation, toolkit creation, and operational tradecraft.

Forensics

Cryptography

Web Exploitation

Reverse Engineering



Binary Exploitation

Security Competitions

Comprehensive List of CyberSec Competitions

ICPC → Intercollegiate Pentesting Competition

NCCDC → National Collegiate Cyber Defense Competition

Types:

- Blue team vs Red Team
- Only deal with a particular branch of Security
- Jeopardy Style

Crypto CTF

PicoCTF

Computer Science

- Lower-level Languages → not portable
- Higher-level Languages → portable

Compilation: Necessary to “run”
Programming Language → You must compile prior to “running”. Set of commands and instruction for the computer to follow. (Bonus points if you say your computer’s OS internal scheduler, I think)

Scripting Languages → You can run without compilation.

All scripting languages are programming languages, but not all scripting languages are programming languages. Why not all scripting languages? Non-Scripting Languages tend to be faster.

Computer Science

Statically Linked (“Statically Compiled”) →

- “Come with everything”
- → Libraries are physically inserted into the executable.

Big Binaries, ‘heavier programs’, prepared

Dynamically Linked →

- “Hopes you have what they need”
- → Pointer to the file of external libraries, but not included.

Little Binaries, ‘lighter’, “*high maintenance*”

Computer Science

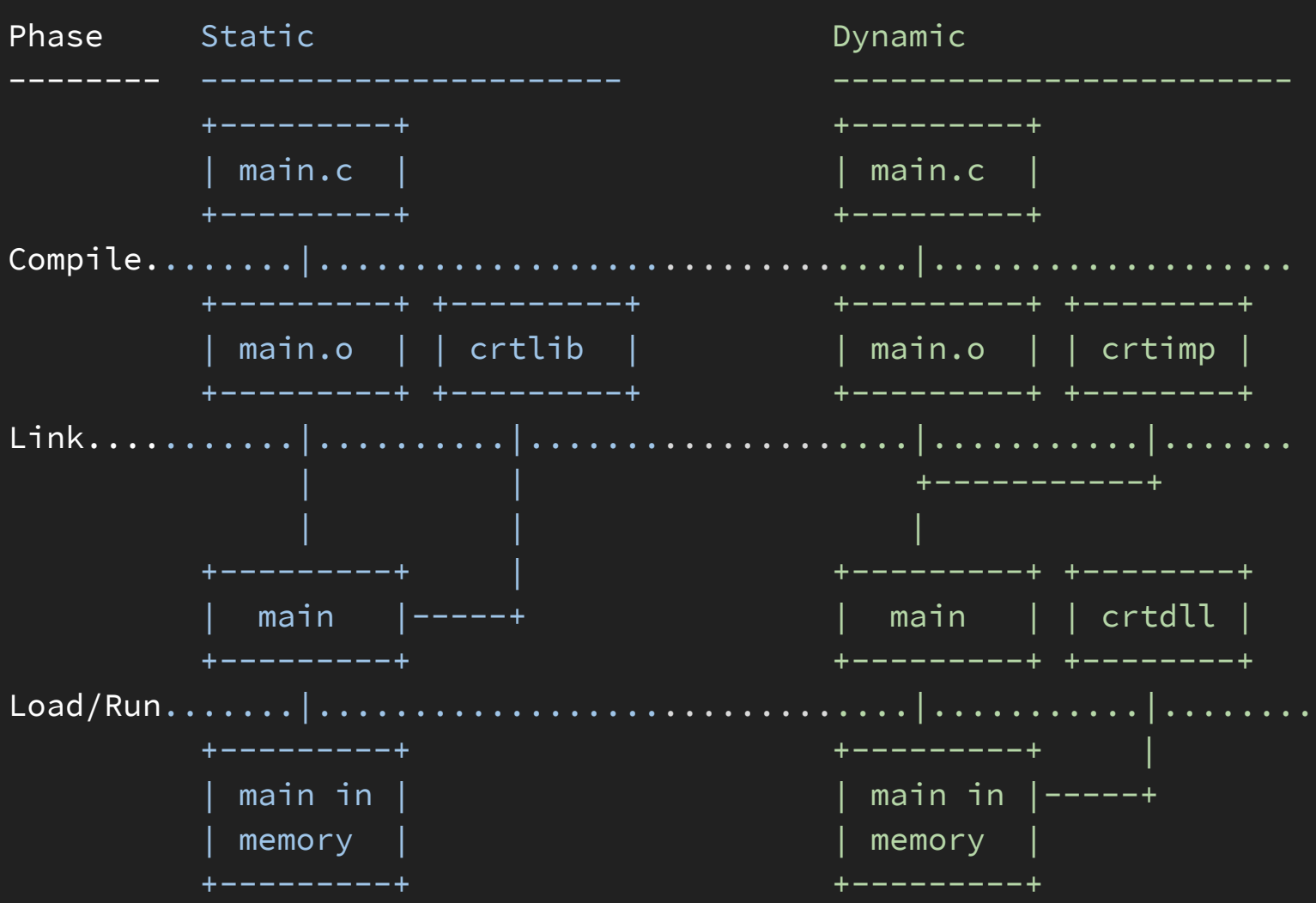
Opinion and you can come at my life

- OOP:
  - Object-Oriented Programming
    - Object this, object that

Code Example

- DDD
  - Data Driven Design
    - Data is data

Code Example


Phase
Static
Dynamic
main.c
main.c
Compile
main.o
crtlib
main.o
crtimp
Link
main
main
crtdll
Load/Run
main in memory
main in memory

What I have seen and heard

Cyber Security Jobs

- Penetration Testing / Pen Testing / TiGeR TeAM TeSTinG / Ethical Hacking
- Security Engineer / Architect
  - Web App
  - Reverse
  - Network
- Security Analyst

~ 75-110k Base Salary

- Factors: Cost of Living, Experience (Years in Industry), Degree (sometimes Presiege Matters), Certs

LIVE DEMO TIME