Final Review Guide
Logistics

- Finals Week Thursday, Dec 8th, 3:00pm - 5:59pm
- In Person @ CENTR 119
- Final will cover everything (focus on the second half)
- Format:
  - True/False
  - Multiple Choice
The Security Mindset

- Threat Modelling (What are we trying to protect, from whom)
  - Security Boundary & Attack Surface
  - Risk assessment
  - Adversarial Mindset

- Security Properties
  - (CIA: Confidentiality Integrity Availability + Privacy)
Low Level Security

- Stack layout
  - Stack, Heap, Data, Text
- Purpose of common registers
  - Esp, ebp, eip, etc.
- Understand Function calls
- Buffer overflows vulnerabilities
  - Format String
  - Heap
  - Integers
  - Pointers
Buffer overflow mitigations

- Stack Canaries
  - Detect overwriting of the return address
- Data Execution Prevention (aka W^X)
  - Make all pages either writable or executable, but not both
- Address Space Layout Randomization (ASLR)
  - Add random offsets to sections of process memory
- Control Flow Integrity (CFI)
  - Protecting indirect transfer of control flow instructions.
- Should be able to describe
  - Their purpose
  - How they work, why can they mitigate
  - How to bypass them, PA2
Buffer overflow mitigations evasion

- Heap spraying
  - Spray heap with many shellcode
- Return-to-Libc
  - Overwrite the return address to point to start of system()
- Return Oriented Programming
  - Make shellcode out of existing application code
- Should know
  - Their motivation
  - What mitigations can they evade
Isolation

- Six Principles of Secure System Design
  - Definition
  - Example
- Process memory isolation
- Unix permission system (ACL and uids)
- User/Kernel Privilege separation
- Virtual memory and Address translation
- Page tables
  - How does it work
  - How do we make syscalls fast, what could go wrong?
Side Channel

- Cache based attacks
  - How does cache work, why cache leave opportunity for side channel attacks
  - Three basic techniques (Evict and time, Prime and probe, Flush and reload)
- Time based attacks
  - Time hack in PA3
- Meltdown, Spectre & Rowhammer
  - General ideas for each.
  - If there's solutions, what?
Crypto

- Encryption
- Cryptographic Randomness
- Symmetric-key
  - Hash Function (MD5, SHA1, SHA2, SHA3)
  - MACs
  - Stream Ciphers
  - Block Ciphers
    - ECB / CBC / CTR Mode
- What property do they give?
- Purpose / limitations
Crypto

- Asymmetric-key
  - Public / Private key
  - Usage
  - RSA encryption
  - Digital Signatures
- Public Key Infrastructure
Crypto

- Web of Trust (e.g., PGP)
- Certificate Authority (CA)
  - TLS
  - Certificate Revocation
- Constructing a secure encrypted channel
- CDNs
- Secure Shell (SSH)
Web

- HTTP
  - Protocol
  - Request / Response
  - Methods
  - Common status code
- Web sessions
- Cookie
  - Purpose
  - How to set and use
Web

- Browser
  - Load and execute content
  - Basic/Nested execution model
  - Frame and iFrame
  - Document Object Model (DOM)
  - DOM and JS
  - Same Origin Policy (SOP)
  - SameSite
Web Attacks and Defenses

- Cross Site Request Forgery (CSRF)
- Phishing
- Server-Side Injection
  - Command injection
  - SQL Injection
    - SQL basics
    - Mitigations
- Client-Side Injection
  - Cross Site Scripting (XSS)
- Content Security Policy
- Understand how the code/attack works
Network

- **Layers**
  - Application
  - Transport
  - Network
  - Link
  - Physical

- **IP**
  - Protocol functioning (Routing, Fragmentation)

- **TCP**
  - 3-Way Handshake

- **TCP/IP Security Model**

- **Other protocols mentioned (ARP, BGP, UDP, etc.)**
  - Purpose and layer
  - ARP Spoofing, BGP Hijacking, TCP Spoofing...
Network

- DNS
  - Purpose
  - Hierarchy
  - Caching

- Attack
  - Cache poisoning
    - Attacker model
    - QueryID
    - Attack itself
    - Defenses
Network

- Basics of defenses (basic idea + pro/con)
  - Firewalls
    - Default allow/deny
  - NIDS
  - Honeypots
- NAT
  - Purpose
  - Pro/Con
- DOS
  - Method
Authentication

- Protecting Password
- Phishing
- Password attacking
- One-Time Passwords
- Biometrics
- Good/Bad Examples + possible attack
Malware

- Virus, works - goals, methodology
- Detection
  - Scanning Signature
  - Integrity checks
  - behavior detection
- Polymorphic malware properties
- Malware outbreak
  - Mitigations? - Network telescopes
- Botnet
  - Architecture
  - Detection
  - Removal
- Spam / Fraud
- Ransomware
- Email spam
  - method
  - Mitigation - blacklisting, Sender authentication
Privacy & Law

- Privacy
  - Tracking
  - Information tracked
  - Value - Ad ecosystem
- TOR (High level)
- Criminal processes for obtaining data
- Rights to privacy
- CFAA, DMCA, etc.