Pentesting Code: Learning from a Case Study

Dr. Jared DeMott
SECURITY RESEARCHER AND ENGINEER

@jareddemott www.vdalabs.com

Overview

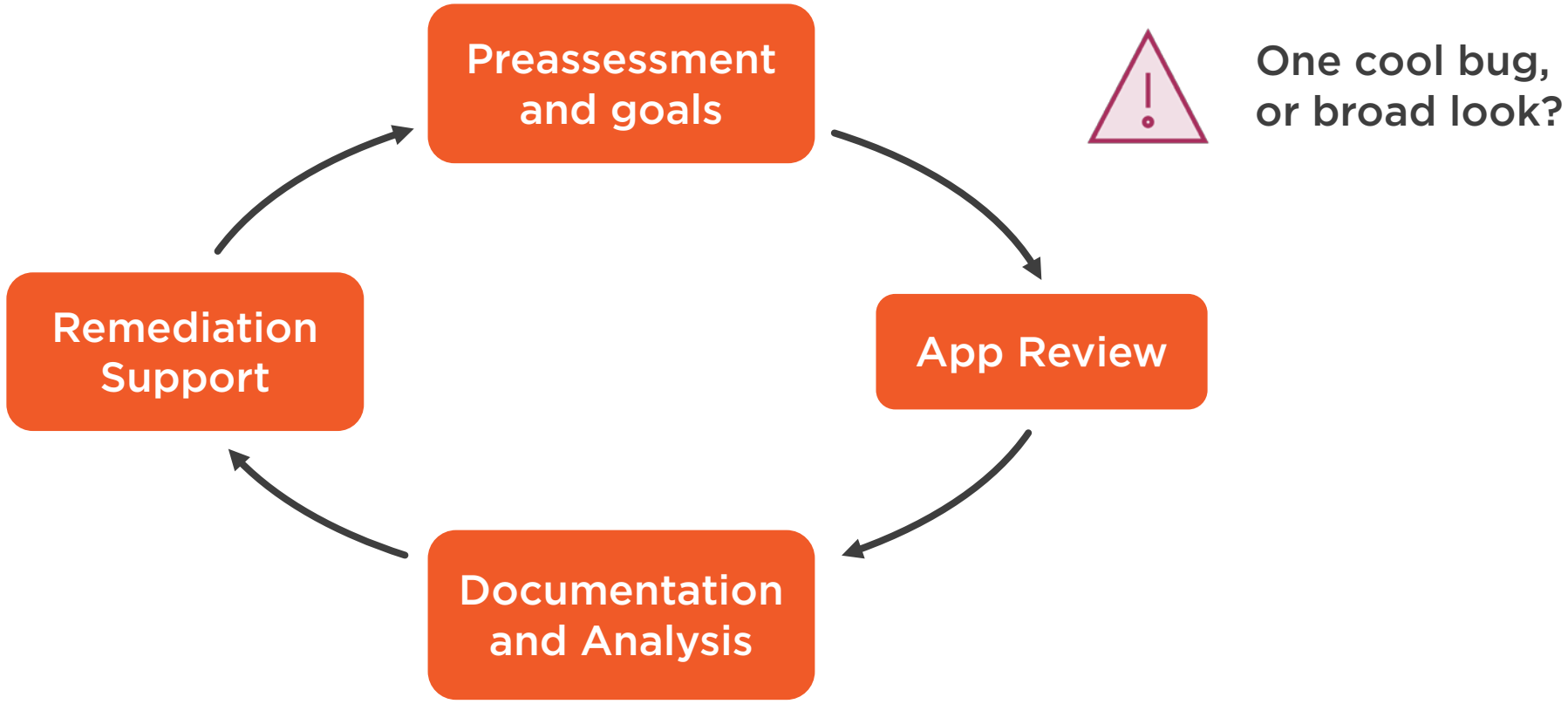
Manual Analysis

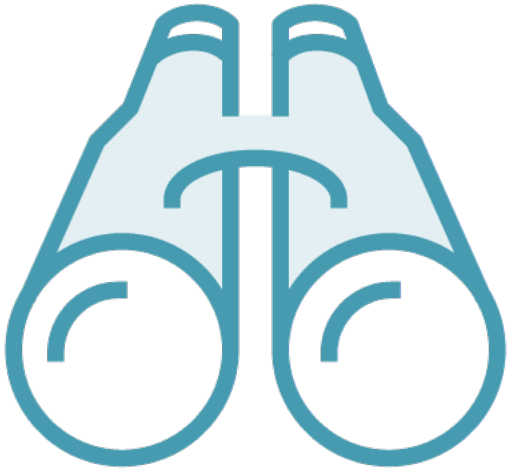
- Process
- Techniques
- Case study

Manual Code Audit

- If you have an expert – use them!
  - Use them to train others
  - Teamwork preferred
  - Some consulting companies specialize in security code audits

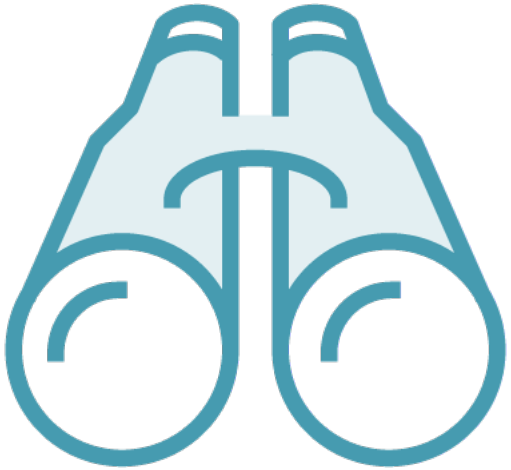
Process Overview





Purpose and Security Expectations

- What is the application suppose to do?

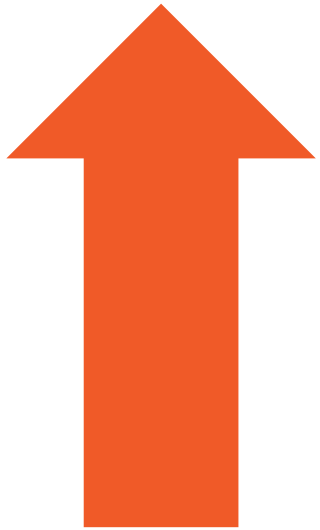


Assets and Entry Points

- Attack surface focused

Techniques

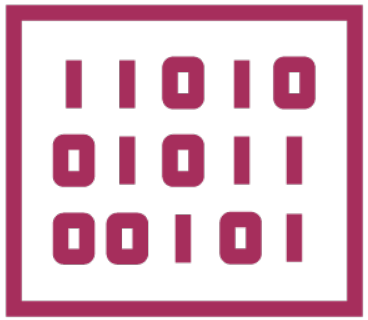
Top down



Bottom up

Techniques

Line-by-line



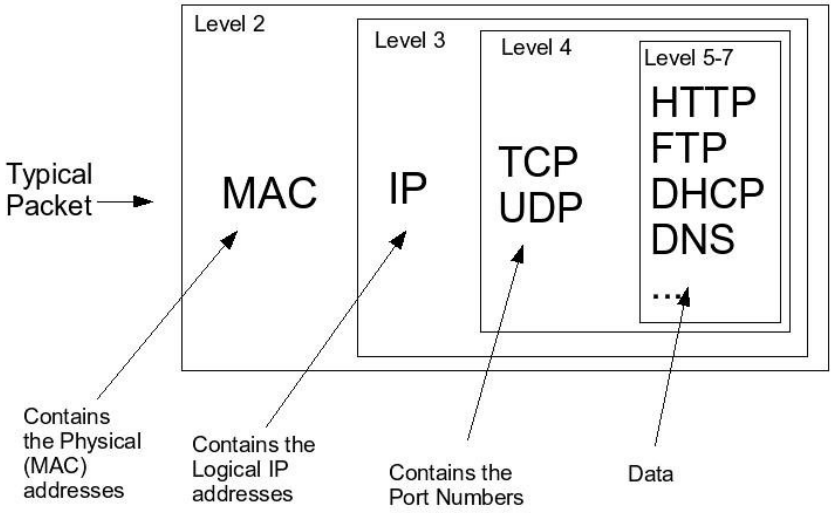
Desk-checking

Multiple Passes

OpenSSH: Preassessment

Buffer Subsystem

buffer.c and bufaux.c



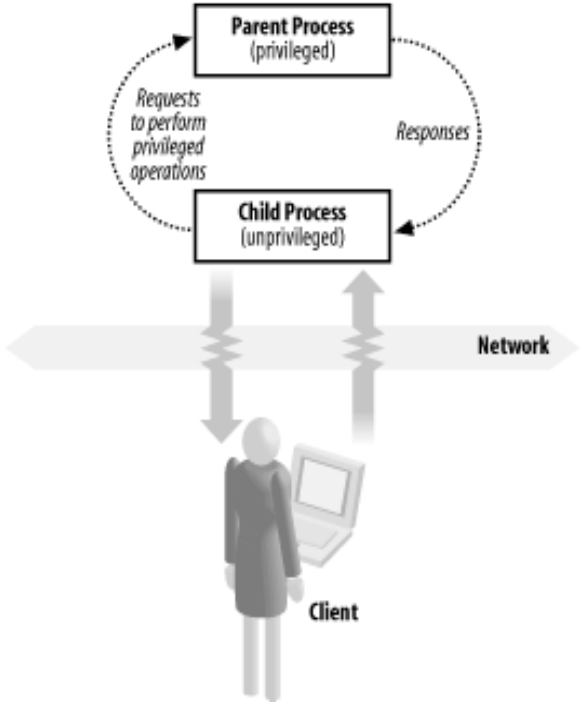
Packet Subsystem

packet.c

OpenSSH: Preassessment

Crypto Subsystem

cipher.c



Privilege Separation Subsystem

monitor.c and monitor_wrap.c

Threats?

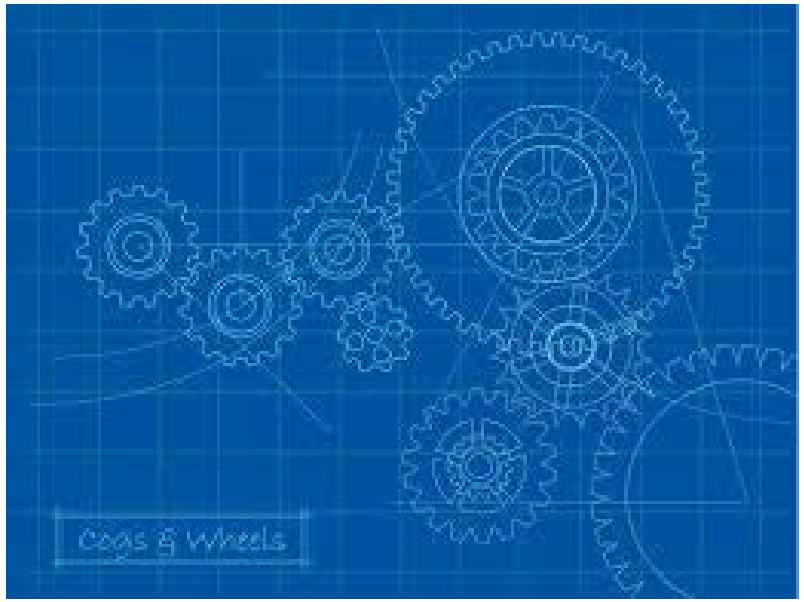
Administrator

Authenticated User

Unauthenticated User

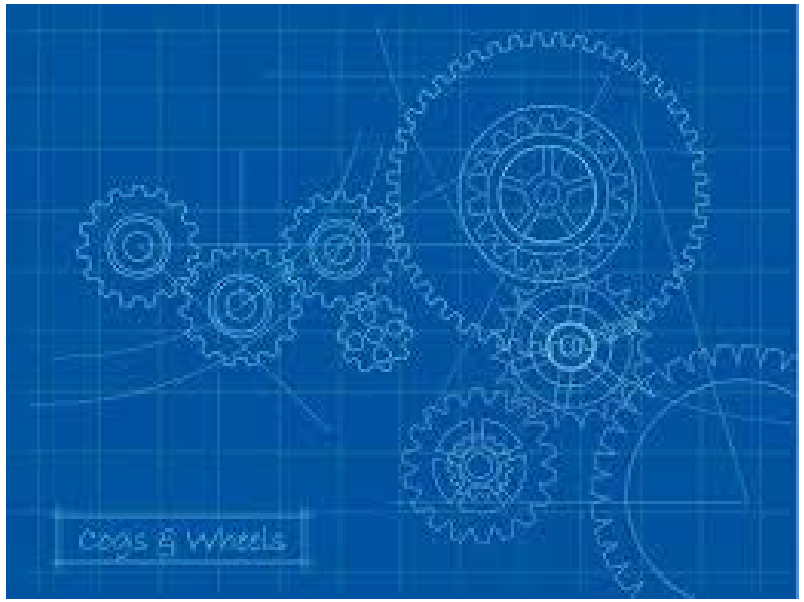
Remote Unauthenticated User

- How to exploit that risk?
  - Low-level packet handing routines
  - Identification exchange
  - Session setup
  - Compression handling
  - Authentication
  - Privilege separation
  - Authentication files
  - External application invocation



Low-level Implementation Analysis

- Consider the viability of each low-level bug class
  - Integer errors
  - Buffer overflows
  - Format strings



Low-level Implementation Analysis

- Design issues for a double free?
  - The *fatal()* function calls *cleanup_exit()*
  - Could this be a problem if something it cleaned up was in an inconsistent state?

High-level Attack Vectors

- SSH Protocol
  - Sniffing
  - Man in the middle
  - Protocol quirks and state

High-level Attack Vectors

- Login
  - Brute-forcing
  - Multi-stage authentication
  - Disabled accounts
  - File-based authentication
  - Incorrectly setup/functioning authentication

Comparing Verification Techniques

	Static	Dynamic	Manual
Scans all code	X		
Hammers attack surface		X	
Finds tricky design and implementation bugs			X
Lower cost	X	X	
Med cost	X	X	
Higher cost			X

Course Summary

AppSec

- Maturing Development Process

Hope to have you in the next course!