

11/1/06

1. Slides on Buffer Overflow
 2. DDOS - paper.
-

Hacker

(1) inexperienced or unskilled at a particular activity — eager to know more about the system

(2) an expert in programming and solving problems

- good at fixing bugs in the system.
 - patch
- create problems

(3) a person who gains access illegally to a system and tampers with information

Jeff Grume

Inside Internet
Security

— What Hackers
Don't Want you to Know
- Addison Wesley (2000)

ISBN- 0-201-67516-1

Editor - Ryan Russell

Hack Proofing
your network (2nd Edition)
- Syngress. (2002)

ISBN - 1-928994-70-9

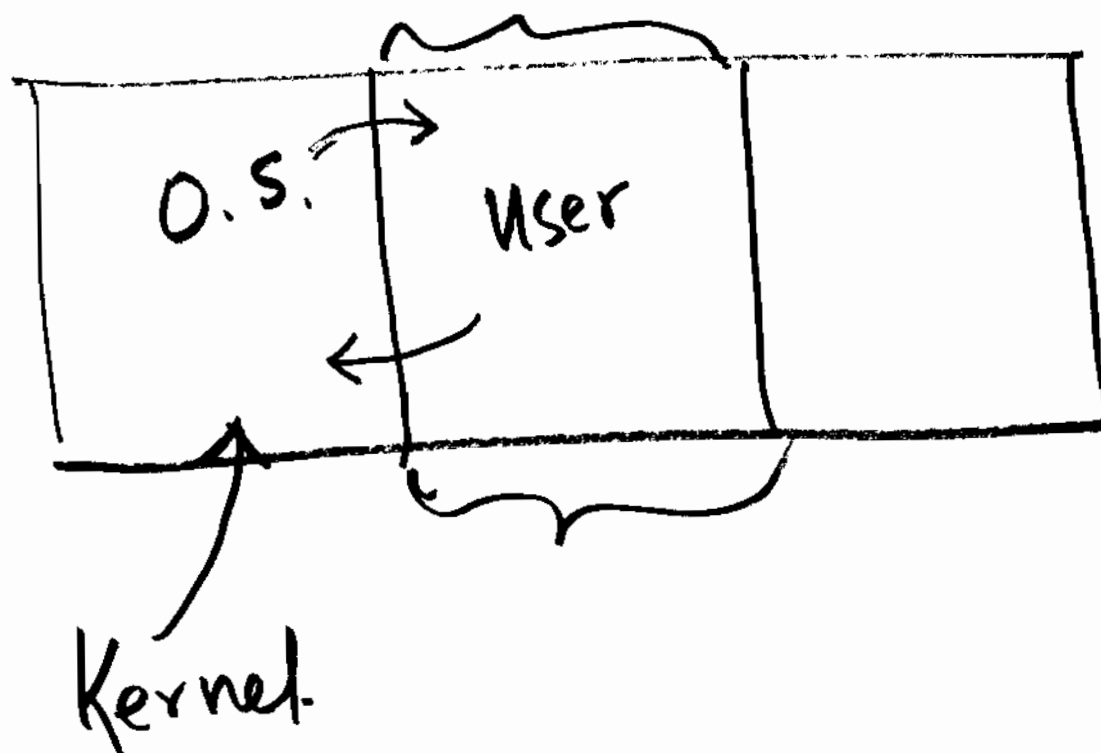
Honey Pots

① Network Protocols.
Peer-to-Peer.

Format

Header	Data
--------	------

② Operating System.
- Kernel
- User.

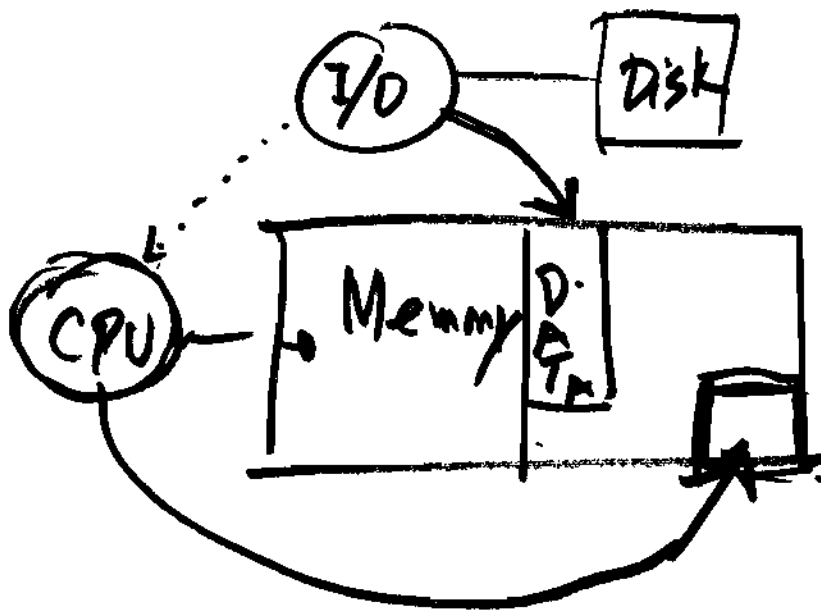


③

Computer Hardware

How does the CPU work?

Interrupt Driven.



④ Database.

Policy

Simple policies.

= Not all simple policies are good but all good policies are simple.

=

(1) in touch with reality.

(2) Single point

(for reporting any violation of the policy)
for warning issuance.

(3) Preserve the crime
scenario.

- Violation.

(4) Backup and recovery

(5) Cost.

(6) People, Policy, Tools.
Environment.

Weakest Link -
- People.

Tools -

Password. = does not give security

guessing.
look over ^{the} shoulder

=
Eavesdropping on network

Software - downlevel.

More time to determine
the flaws in the design

Virns - Harmless - (no
Back door - harmless
attack)

Vulnerability & Audit

Chapter 20

Chapter 21.

Vulnerability

The specific failure of the controls is called vulnerability (or security flaw)

Design of the software
Design of the hardware

Formal approach.

Preconditions



~~Program~~ Software

↓ Postcondition.

Penetration testing.

Red Team.