lecture 0-0: computer security overview

<http://www.securityfocus.com/>

Attack (hacker's hut: <http://www.win.tue.nl/~aeb/linux/hh/hh.html#toc10> )

Information collecting

sniffing: collect info on packet data

scanning: collect info on live ports

Breaking into the target system

brute-force: password guessing

unexpected input: buffer overflow, SQL injection, Cross-Site Scripting,

format string, integer overflow, …

unexpected behavior/protocol: MIM, application vulnerabilities, java vulnerabilities

social engineering

Control the target system

malware, ransomware, spyware : install attacker’s program

kernel hacking : modify the kernel (LKM)

Block/Destroy target system

DoS, DDos

Defense

Detect/block the attack

detect scanning

detect attack packet: IDS

block port: firewall

Make system/protocol/application secure

encryption, secure os, SSL(secure socket layer), secure programming

Trace the attacker

logging, ip trace, computer forensics