Computer Network Defense

defensive operations
- what can we do to "protect" ourselves?
- one option is to encapsulate our services/OS
  - virtualization (virtual machines)
    - virtualbox
    - vmware
    - xen
  - chroot jails

defense in depth
- don't depend on a single mechanism for protection
- layered approach (multiple layers of defense)
- idea: use several varying methods
  - e.g. anti-virus on firewall but also anti-virus on machines downwind
- military: delay rather than prevent
  - yield space in order to buy time
- so it should prevent security breaches
  - while giving time to respond
- can we draw parallel to DFS?

defense in breadth
- many aspects can exploit vulnerabilities
- we need to cover all of these
  - e.g. email security and messaging security and anti-virus and spyware, etc
- can we draw parallel to BFS?

IDS/IPS
- how can we detect intrusions?
- how can we detect attackers?
- could we protect/prevent in addition to detect?
- tcp wrappers
  - maybe we can think about this being like a filter for tcp packets
  - we can scan, log, anonymize, etc
  - and maybe we could detect/protect/prevent via tcp wrappers

PDR^3 (or should it be PDRER?)
- prevent
  - we're a "pill" society
    - we prefer to take care of the symptoms, not the cause
    - and that's a bad idea (but a money-making one!)
  - better idea: identify the case and prevent the problem from occurring again
    - but that takes work (effort) – that's why we're a symptom society
    - we're lazy people when you think about it
  - so best case is to prevent security breaches and vulnerability exploits
    - but that's not always possible, particularly in cyberspace
  - tools:
- detect
  - if we can't prevent, we must find out when we have a problem
  - ids, ips, ips
  - firewall, patches, anti-virus (triad)
  - tools:

respond
- if we detect, we can't just let something bad happen
- what to do, what to do?!
- how proactive can we be?
  - do we just secure our system and repair?
  - then prevent the perpetrator from doing it again (how?)
  - can we “engage?”
  - can we find out who did this and where they live?
- Tools:

recover
- if our system was compromised, we may need to recover
- how might we do this?
- or might we endure instead of recover? or both?
- tools:

restore
- maybe our system is irrecoverable
- so we take this as a learning experience
- we restore from some previous backup
- then we look at how to prevent this from happening again
- and we loop back to the beginning...

avoid?

ddos
- dos: denial of service attack
  - attempt to make computer resources unavailable
- ddos: originates from multiple systems
- how?
  - consume computer resources (bandwidth, cpu, disk space)
  - disrupt configuration information (e.g. routing information)
  - disrupt state information (e.g. reset tcp sessions)
  - disrupt physical network components
  - obstruct communication
- smurf attack (ping flood)
  - generate a lot of network traffic on a network
  - by flooding the target system with spoofed ping messages to broadcast addresses
- syn flood
  - SYN, SYN-ACK, ACK, hang up
  - half-open connections may take up resources on the client
- ping of death
  - normal ping packet size is 56 or 84 bytes
  - sending one that is larger than max ip packet size (65,535 bytes) could cause a crash (old)
- pdos: permanent dos
  - phlashing (illegitimate flashing of hardware → bricks the device)
- application level floods
  - irc floods
  - buffer overflow
  - banana attack: redirect outgoing messages back to sender
- degradation of service
  - many zombies mount temporary dos
  - harder to detect
- some are unintentional (google news on the day of michael jackson's death)

backscatter
- some attackers spook source ip
- you respond as usual
- those response packets are backscatter
- imagine if i spoofed millions of packets with your address as the source?

network telescope (darknet, internet motion sensor, black hole)
- used to take a look at the unused part of the Internet
- all traffic to these addresses is suspicious

botnet
- a bunch of zombies!
- software agents that run autonomously and automatically
- mostly interpreted to be malicious
  - but can be legitimate
- compromised via
  - drive-by-downloads (RTFM!)
    - awareness is important (in everything actually)
  - browser exploits (IE6)
  - worms
  - Trojans
  - backdoors
- bot herder/master established C3
  - often takes place on IRC server
  - usually runs hidden in a covert channel
- Dutch police found a 1.5 million node botnet!
- used in many ways and typically auctioned to highest bidder
  - spam
  - ddos
  - click fraud
  - adware
  - spyware

script kiddies
- those who use scripts or programs developed by others to attack computer systems
- most “hackers” are actually script kiddies
- tools
  - winnuke (dos)
  - back orifice (remote system administration)
  - netbus (remote system administration)
  - sub7 (remote system administration)
    - netbus backwards and then substitute 7 with ten
    - 1/1/2010: hacker took them down (still down and closed forever)
  - metasploit (os computer security project)
  - prorat (backdoor Trojan)
  - and more...