DDoS

Jeff Chase
Duke University

Flood Attacks

- Direct a stream of packets toward a victim.
- Require the victim to do work per packet.
  - Classic: TCP SYN floods (2000pps sufficient)
  - ICMP floods
- Victim has insufficient resources left over to perform useful functions.
- Tools are out there:
  - WMDoS genie is out of the bottle

Taxonomy

- Single-source vs. “botnet” of zombies.
  - Zombies are good systems (e.g., yours) that have been penetrated and compromised.
  - Often a pathogen or trojan that leaves a back door for the attacker to use it as a proxy.
- Randomly selected victim vs. targeted (vendetta)
- Undisguised vs. IP spoofing of source address.
  - IP-spoofed source address randomly selected
  - Often generates backscatter from victim to spoofed source.
- Direct vs. reflector
  - In a reflector attack, the backscatter is the attack traffic.
    - Focus the backscatter

Intelligence Gathering

- Honeypots and honeypot farms
  - Set up idle machines that present an attractive target to an attacker looking for zombies.
  - Most zombies are recruited by randomly sampling the IP address space: they will find you.
  - Honeypot operation and ethics?
- Network telescopes
  - Most spoofed source addresses are randomly selected from the IP address space.
  - Set up idle machines that listen for backscatter traffic on a sample of the address space.
- IPv4 has a small address space
  - What would be the effect of IPv6?

Countermeasures

- Limit effectiveness (don't become a victim)
  - Firewalls
  - TCP cookies
    - Don't do the SYN work until the SYN-ACK-ACK.
    - Why doesn't the attacker just respond to the SYN-ACK?
- Suppress attacks (don't be used as a weapon)
  - Good hygiene: don't become a zombie.
  - Ingress filtering to suppress disguised attacks.
    - Edge routers detect spoofed source addresses originating from a stub network.
  - ACC and Pushback: suppress attack in transit.
- Accountability and legal sanction
  - IP Traceback

Another Countermeasure

- “Encourage” others to use good hygiene.

Subject: you are vulnerable
From: you@yourmachine.yourhome.com
To: you

Greetings,

This is a message from your local white hat hacker. I own you. I can do anything you can do on your machine. Fortunately for you, I am your friend….

Ethical?