Analysis of the December DDoS Attack Against SCO

Colleen Shannon (CAIDA)
David Moore (CAIDA/UCSD-CSE)

cshannon @ caida.org
dmoore @ caida.org
www.caida.org
Network Telescope

- Chunk of (globally) routed IP address space
  - 16 million IP addresses
- Little or no legitimate traffic (or easily filtered)
- Unexpected traffic arriving at the network telescope can imply remote network/security events
- Generally good for seeing explosions, not small events
- Depends on random component in spread
Network Telescope: Denial-of-Service Attacks

- Attacker floods the victim with requests using random spoofed source IP addresses
- Victim believes requests are legitimate and responds to each spoofed address
- We observe $1/256^{th}$ of all victim responses to spoofed addresses [MSV01]
SCO Denial-of-Service Attack

• Who is SCO?
  – UNIX (linux) software company
  – Originally Santa Cruz Operations
  – Caldera bought Unix Server Division from Santa Cruz Operations in August of 2000
  – Caldera changed its name to "The SCO Group" in August 2002
  – Sued IBM in March 2003 claiming that IBM misappropriated its UNIX operating system intellectual property (acquired from Novell)
  – Threatened lawsuits against many others
SCO Denial-of-Service Attack History

- May 2003
  - SCO gets hit by its first major DoS Attack
- August 2003
  - SCO gets hit by its second major DoS Attack
  - Some rumors that an internal network problem was publicized as a DoS attack
December SCO Denial-of-Service Attack

- December 10, 2003 3:20 AM PST
  - an ~340 Mbit/s SYN flood incapacitates SCO's web server
- December 10, 2003 1:37 PM PST
  - groklaw.net blog "reports" on rumors that SCO is not being attacked; they are faking the whole thing to implicate the open source community
- December 11, 2003 2:50 AM PST
  - the SYN flood is expanded to target SCO's ftp server in addition to their webservers
- December 11, 2003 noon PST
  - SCO takes themselves off the 'net while pursuing upstream filters to block the attack
SCO Denial-of-Service Attack
Now it gets interesting…

- We published http://www.caida.org/analysis/security/sco-dos/

- CAIDA webserver gets a DoS attack of its own
  - 11pm-1am PST
  - Some attack characteristics point to the same perpetrator (or simply same attack tool) but no conclusive evidence
SCO DoS Attack "Results"

- Security experts (us included) need to be careful what they say in the absence of details
  - Sure, technology exists to thwart SYN floods, but not at 340 Mbit/s inbound coming to a DS3
- It's no fun to be a SCO network admin
  - your own ISP won't admit they give you connectivity, let alone corroborate the attack reports
  - your CEO is quoting the aforementioned security experts who say any 5 year old could stop the attack
  - your only hope is upstream ISPs helping you, but your company is not popular with NOC employees
Points to ponder...

• Why did folks believe SCO was faking the attack?
  – What real motivation do they have to implicate the open source community?

• Is it in the best interest of the open source community to say that SCO faked the attack?
  – Encouraging open source advocates not to cheer the SCO DoS attacks is a good plan
  – Wildly accusing SCO of faking attacks or paying others to attack them is counter-productive
The Real Take-home Message

- Many DoS attacks are short-lived pranks, but the potential for real (fiscal etc.) damage from a well-timed attack is great
- What happened to SCO can happen to your customers – and they will want solutions
- Pertinent questions:
  - Will you have a legal obligation to block traffic for your own customers or customers of other ISPs?
  - What about DoS attacks as blackmail or retaliation? For customers? For small ISPs?
  - Could you offer a pre-emptive blocking service? DoS attack “insurance”?
More Information

• SCO writeup:
  – http://www.caida.org/analysis/security/sco-dos/

• DoS attacks:
  – http://www.caida.org/outreach/Papers/2001/Backscatter/

• Network Telescopes
  – Research potential:
    http://www.caida.org/analysis/security/telescope/
  – Practical uses and how to build your own:
    http://www.caida.org/outreach/presentations/2003/lisa_telescope03/

• CAIDA research
  – http://www.caida.org/