Recent Attack Technologies

Neil Long

OxCert

Introduction

- Hope for audience participation!

- At least two aspects
  - Target payloads
  - Attack origins
- Future? arenas

Attack Payloads

- Buffer overflow
- Format strings
  - Any experts in the audience?
- Network DoS
  - volume vs. content

Buffer Overflow

- Kernel switches, defences
- stack vs heap vs libc
- Options off by default

Format Strings

- Relatively recent - major examples
  - Wu-ftpd - Linux
  - rpc.statd - Linux
  - telnetd - IRIX
  - Local uid to root exploits

Built-in Defences?

- Libc modifications
  - Are they enough?
- POSIX compliance
  - LibC from major vendors??
- Source code re-writes
  - continuous release of new exploits

Bugtraq

- Libc
- Imp
- Envcheck klogd
- Cfengine
- rpc.statd improved

- Sperl
- pam_smb and pam_ntdom
- wu-ftpd new variants
- Su
- Php

- Screen
- Sysklogd
- Traceroute
- Ncurses
- Apache mod_rewrite

Attacks

- Scanning granularity
- Real-time IDS
- Post-event IDS
- Multi-source attacks
  - scan host
  - exploit host
  - intrusion host(s)

Tools used

- Root-kits
- hidden ‘extras’
- rapid evolution
- IRC still major factor

Counteractive Tools

- LSOF
- TCT
  - mactime
  - lsi & icat
- Netflows
- Active IDS

DDoS tools

- Trinoo still popular - evolving
- Stacheldraht
- ‘TFN3K’ very worrying
- Trinity (Entitee)
- Handler-agent communication differences

DDoS Payloads

- UDP volume
- TCP SYN flood
- Smurf & Fraggle amplifiers
- Stream
- Fragments and others?
- Higher bandwidth will make them more effective

IP Spoofing

- All vs. partial vs. none at all
- Generator efficiency
- benefits to *them* (and *us)*

Locating the intruder

- Traceback
- Mobility becoming easier - locating more difficult
  - e.g. Use of non-contract cell phones
- Wireless networks
  - promiscuous mode?

New targets?

- Voice-over-IP?
- DNS revisited
- WAP

What is to come?

- DDoS Net of nets? How long?
- Pipes get fatter -
  - firewalls & IDS fall behind?
  - Cost prohibitive?
- Disks keep getting bigger

Finally

- Story is not changing -
  - Demand for fatter pipes, bigger faster machines
  - But security is still an after-thought
- Less logging by ISPs?
- Growing awareness == more incidents
  - increased IRT load
- Liability issues on the horizon?