Security Vulnerabilities and Precautions

Andrew Sansum

29 September 1998

How They Get In

- From outside:
  - System daemon vulnerability
  - System mis-configuration
  - Steal, guess or sniff a password
- From inside
  - File permissions
  - System Vulnerability

What do They do Once In

- Install sniffer
- Install rootkit (SUN & Linux)
- Install Backdoor
- Create DummyID (e.g. root2 or bloggs)
- Erase traces from logs
- Software serving
- Lots else probably - who knows

Scanning Technology

- Full depth: satan, saint and nessus
- Port scans: lots! Best now is nmap with lots of stealth options: SYN, FIN, FTP..
- Specialist scanners like mscan can do many sites, looking for well known vulnerabilities.
- Internal “scan”: COPS and tiger
- Typically see 5-10 scans each weekend

Securing Your Systems is easy!

- Block insecure ports at router / firewall
- Follow the AUSCERT checklist
- Don’t forget the patches!
- Use the scanners described above to double check.
- Internal check with COPS
- Crack the password file

Intrusion Detection

- Connection monitoring at firewall
- Packet sniffer
- High level of system logging
  - TCP wrappers
  - loginlog
  - scanlogd
  - audit daemon
  - portmapper
- Remote syslogd and swatch

Recovery after an Incident

- Checksums are vital
- Promiscuous mode checkers
- Detailed and trusted logs
- Your own sniffer logs would help
- Good system backups
- Know who are valid users!
- Have a plan in place before the incident

Keeping Up to Date

- Using our own eyes!
- Bugtraq and Rootshell
- Specialist advisories: uniras is good
- CERT advisories
- Vendor Patches (last of all!)