Small & Large Networks

- Differences between host & network audits
- What to look for when auditing
- Tools used
- Networks and **NETWORKS**

Differences Between Host & Network Audits

- Change from tactical to strategic thinking
- Mountains of audit information to digest
- Networks are less understood than hosts
- Complexity is far greater; interactions kill
- Instead of SA's, you have **domain** SA's
- You have incomplete data
- Lots of uncertainty

You have incomplete data

- Simply getting a count of machines is difficult
- Finding who is in charge can be arduous
- Hardware breeds like rabbits
- The web of trust often extends outside of your domain
- Not everyone will cooperate
- Audits are much less precise

Mountains of information to digest

- **Must** understand how the network is used
- Serious audit reduction becomes a necessity
- Prioritize - examine key hosts and areas
- Random spot checks

What to Look for When Auditing

- Policy
- Connections to the outside world
- Trust
- Key hosts
- Overall inventory of hosts
- Filesystem sharing (NFS, AFS, etc.)
- Network maps (password, NIS)

What to look for When Auditing (cont.)

- Traffic
- User flow
- Network ACL stuff (packet screens, wrappers, etc.)
- Remote execution bugs
- Authentication methods
- Significant hardware/software
- Data leaks

Connections to the outside world

- Perhaps the second most important thing
- Modems
- X.25
- TCP/IP
- UUCP
- Sales offices/insecure sites

Trust

- Servers vs. clients
- DNS
- Packet filters
- NIS
- IP

Key hosts

- Interview different personnel to find them
- Critical functionality or sensitive info
- Understand how they fit into the network
- Should gather extra host audit data
- Be **extra** careful of trust

Traffic

- Examine the flow - what, where, when
- What type (TCP/IP, IPX, appletalk, etc.)
- Cleartext/encrypted
- Do screens or network ACL's get any hits?

Significant Hardware/Software

- Kerberos
- Smart hubs
- Homegrown/specials

Tools used

- Host audit tools
- SATAN/ISS
- tcpdump
- Sun Net Manager
- War Dialers

Networks and **NETWORKS**

- Takes a LONG time to prepare
- Takes a LONG time to examine
- People make things even harder
- You get blamed for odd things

Networks and **NETWORKS (cont.)**

- A control freak's nightmare
- 99% of hosts play very little role
- you will **NEVER** have a truthful picture
- inventory is always wrong
- You can't get good host audit information

Networks and **NETWORKS (cont.)**

- External connections are very hard to map
- trust maps are extremely difficult
- Network and host administration is very different by location