Host Security

1

Host Security: Pro

- Maintaining strong security on host avoids the “crunchy shell around soft, chewy center” problem
- If perimeter security fails, network is often wide open to attack
- May rely on vendor-provided security features

2

Host Security: Con

- Vendors slow to respond to security holes
- Effort scales with number of hosts being protected
- Requires constant upkeep
- Reduces host-to-host trust or increases dependency on common security policy between peer hosts

3

Network services

- Historically, bugs in network servers are a major weakness in networked systems
- Turning off unnecessary services is desirable
- Turning off services may be difficult and vendor specific

4

Reducing services

- (most systems) Edit /etc/inetd.conf
- (BSD systems) Edit /etc/rc and /etc/rc.local
- (SYSV systems) Edit or delete entries in inittab and /etc/rc.d
- Check process table and output from netstat. Reboot system, make sure it boots OK, and repeat

5

Ident

- Attempts to get advisory information about originating user of connection
- Requires daemon running on remote client system
- Not high quality authentication
- Useful for backtracking attacks

6

Password files

- On many UNIX systems password files are world readable
- Easy to attempt dictionary attacks
- If at all possible use shadowed password files
  - Not a solution but it's better than nothing
- Securely distributing password files is a hard problem

7

Yellow pages/NIS

- Minimal security
- Within network it is easy to download a system's password file
- If using NIS for passwords make sure that NIS access is blocked from Internet

8

Npasswd

- prohibits users from choosing easily guessed passwords
- Many O/S require minimum password lengths or use of at least one “special” character

9

S/key

- One-time authentication system based on multiple invocations of hash algorithm
- May be used with hardcopy password lists
- May be computed on laptop
- Available: ftp://thumper.bellcore.com/pub/nmh/

10

Host Security Tools

- Expert
  - Tools “know about” and look for problems
  - Based on past experience
  - Won’t recognize “magic” security holes
- Audit and Monitoring
  - Good for damage control
  - Useful for identifying well-known attacks in progress

11

Host Security Tools *(cont)*

- Reactive
  - Maintain information about proper state of system and identify deviations from the norm
- Information Security
  - Deny an attacker useful information
  - This is NOT the same as “security by obscurity”

12

Expert Tools: COPS

- COPS contains heuristics of common system weaknesses
- Analyzes:
  - File ownership, Directory ownership, Device ownership, User's *.rhosts* files, etc, etc, etc...
- Does a good job of finding well-known holes

13

Expert Tools: ISS

- ISS: Internet Security Scanner - scans for known host networking software weaknesses
  - Domain names
  - Common login names
  - RPC portmapper reachability
  - NFS reachability
  - Sendmail debug hole, etc, etc, etc...

14

Expert Tools: STROBE

- Super-Optimised TCP Port Surveyor
  - locates and describes all listening (open) TCP ports on one or more remote hosts
  - approximates parallel finite state machine
  - can port scan entire subdomains
- Can be used in tandem with ISS

15

Expert Tools: SATAN

- System Administrators Tool for Analyzing Networks
- Easy to use graphical interface
  - searches widening circles of subnets
  - uses DNS information
  - three scan modes: light, medium, heavy
    - heavy generates *serious* ICMP traffic, can crash some systems

16

Commercial Tools

- Netprobe
  - Runs up to 85 tests per host
  - 2 modes, noisy and quiet
  - New offering from Infostructure Services & Technologies
- Pingware
  - Analysis tool similar to SATAN
  - Delivered as consulting service by Bellcore

17

Expert Tools: Crack

- Expert tool used for identifying “weak” passwords
- Attempts to find matching encryptions using a large dictionary
  - Typically approximately 5% of any given password file is guessable
  - Used by systems administrators to scan for weak passwords and warn users

18

Audit Tools: Gabriel & Courtney

- Anti-SATAN early warning systems
- Courtney developed by CIAC at Lawrence Livermore Labs
  - uses tcpdump to count number of new services a machine originates within a certain time window
- Gabriel distributed free by Los Altos Technologies

19

Expert & Audit Tools: TAMU Toolkit

- Developed in response to campus-wide breakins in August of 1992
- Suite of tools for packet filtering, network monitoring and system “cleanup”

20

Drawbridge

- Part of TAMU Toolkit
- Packet filtering firewall package controls access on a host-by-host and port-by-port basis at T1 speeds
- Use of compiled tables allows very complex filters with little penalty
- Compromise between security and flexibility

21

Tiger Files

- Part of TAMU Toolkit
- Designed for ease of use - can be run by end users on own machines
- Includes checks for
  - mail aliases and cron jobs
  - password file discrepancies
  - file permissions (maintains database)

22

Netlog

- Part of TAMU Toolkit
- Advanced sniffer system for network monitoring
  - tcplogger
  - udplogger
  - netwatch
- TCP & UDP loggers for SunOs 4.x only

23

SPAR

- Part of TAMU Toolkit
- Show Process Accounting Records
- An offspring of the “extract” utility
- Much faster than *lastcomm*

24

Audit Tools: Swatch

- "System Watcher" scans for known patterns in system logs
- Invokes specified filter when pattern is detected
  - Warns about multiple failed logins
  - Warns about bad SU attempts
- Can send alarms via email or pager

25

Audit Tools: Watcher

- Maintains saved state of system files or output
- Notifies administrator when boundaries are exceeded
- Examples
  - Disks filling up
  - Processes running wild
  - Defunct processes

26

Audit Tools: UNIX Accounting

- UNIX accounting tools maintain timestamped records of program execution
- May be extremely useful for tracking intruders
- Process accounting enabled for chargeback purposes may “finger” bad guys

27

Audit Tools: TCP_Wrappers

- Log connections to TCP and UDP services
- May selectively permit or deny based on originating host
- Useful for restricting service as well as audit
  - May help detect port sniffers
  - May help detect NFS probers

28

Audit Tools: ARPWATCH

- Monitors ethernet activity
- Keeps database of ethernet/IP address pairings
- Uses tcpdump, and libcap, an LBL interface for user level packet capture
- Developed at Lawrence Berkeley Labs

29

Reactive Tools: Tripwire

- Builds cryptographic checksums of system
- May be stored on write-protected media
- Re-running checksums will list all files that have changed since last scan
- Effective at finding trojan horses or trapdoored programs after breakins

30

Reactive Tools: Archives

- Checksumming will only tell you that a file has changed
- Archival media let you determine exactly *how* it changed
- Backups are useful for security as well as crash recovery
- Some sites save copies of important files and compare them nightly

31