Internet Security Overview

Dave Safford, Texas A&M University

Presenter:

Dr. Dave Safford, Director
Computing and Informations Systems
Texas A&M University

Internet Security Overview

Dave Safford, Texas A&M University

Abstract

- Problem
- Goals/Policies
- Approaches
- Resources
- References
- Questions

- Postscript copy of this presentation available from net.tamu.edu:pub/security/TAMU/e-comm.ps

Internet Security Overview

Dave Safford, Texas A&M University

Problem:

- internet hacker underground
- typical unix workstation misconfigured.
- sniffing (weakest link)

- => unprotected sites are at grave risk
- If you don't protect yourself, you will be broken into.

- Examples:
  - TAMU breakins August 92
  - UT breakins
  - Rice breakins

Costs:

- availability hit (down time to fix systems)
- confidentiality hit (read everything)
- integrity hit (some malicious data destruction)
- high manpower costs to recover

Internet Security Overview

Dave Safford, Texas A&M University

Goals/Policies:

- 3 T's
  - integrity
  - confidentiality
  - availability
- Security vs Convenience spectrum

Approaches:

- Firewalls
- Network Monitors
- Host Checks

- Passworded Dial-ups
- "Secure" twisted pair ethernet hubs
  (we use 3-COM FMS-2 stackable)
- Backups

Firewalls:

- None
  - easy, but you'll regret it
- Simple router filters (r'cmds, yp, nfs, tftp, X)
  - low cost, easy to implement, fairly invisible
  - only fair security improvement
- Powerful filters (Firewall-1, drawbridge)
  - medium cost, low visibility, medium security
- "true" proxy firewalls
  - high cost, high visibility, high security
- air-gap
  - total security, poor functionality

Network Monitors:

- TAMU's netlog:
  - tcplog
  - udplog
  - netwatch - intrusion detection
    - telnet, ftp, rlogin, rshell, smtp, tftp, sunrpc, FSP

Netwatch Example Output

```
09/16/93 01:29:43.63 [rpc] x.y.4537 HOST.TAMU.EDU RPC
                lookup for: ypserv

09/16/93 01:36:23.80 [rpc] x.y.4565 SUN.TAMU.EDU RPC
                lookup for: ypserv

09/19/93 11:24:13.89 [ftp] a.b.1025 PLANET.TAMU.EDU
                'anonymous' (u@a.b) unknown cmd:
                cat ANNOUNCE

09/19/93 14:41:38.11 [rpc] SUN.TAMU.EDU.4552 r.m.com RPC
                lookup for: rexd

09/20/93 22:52:48.70 [telnet] d.e.1090 VMS.TAMU.EDU
                attempted login as 'field'

09/20/93 22:52:48.77 [telnet] d.e.1090 VMS.TAMU.EDU
                failed login as 'field'
```

Host Checks:

- TAMU's tiger scripts
  - easy to use, with detailed messages and explanations
  - security configuration auditing
  - security patch verification
  - intrusion detection

Overview of Checks

- login accounts
- anonymous FTP
- NFS exports
- inetd configuration
- .netrc files
- PATH setting
- file permissions
- digital signatures
- embedded pathnames
- e-mail aliases
- cron files
- group file(s)
- known break-in signs
- passwd file(s)
- printcap file(s)
- .rhosts files
- file system scan

Resources:

- Organizations:
  - CERT
  - FBI
- Mailing Lists: (send "subscribe" in body to majordomo@)
  - Firewalls@greatcircle.com
  - Academic-firewalls@net.tamu.edu
- Newsgroups:
  - comp.security.announce (CERT)
  - comp.security.unix
  - alt.security

Resources:

- Major FTP sites:
  - ftp.cert.org
  - coast.cs.purdue.edu
  - net.tamu.edu

Vendors:

- Sun - igateway
- DEC - SEAL
- ANS - Interlock
- TIS - Gauntlet

- Checkpoint Technology - Firewall-1

Free Tools:
(available from coast.cs.purdue.edu:/pub/tools)

- tcpwrapper
- TIS-toolkit (coast.cs.purdue.edu:/pub/mirrors/ftp.tis.com)
- socks
- TAMU
  - drawbridge
  - tiger
  - netlog/netwatch
- cops
- tripwire
- crack

Publications:

- Rik Farrow, "Barbarians at the Walls", Open Computing, Oct, 1994 pp 62-65.
- Dan Farmer, "Improving the Security of your Site by Breaking into it", (coast.cs.purdue.edu:/pub/doc/firewalls admin_guide_to_cracking)
- Safford, Schales, Hess, "The TAMU Security Package: An Ongoing Response to Internet Intruders in an Academic Environment", Proceedings Fourth USENIX Security Symposium, Oct 1993, pp. 91-118. (Also available via ftp from net.tamu.edu:pub/security/TAMU/tamu-security-overview.ps.gz)
- Cheswick, "The Design of a Secure Internet Gateway", coast.cs.purdue.edu:/pub/doc/firewalls/ Bill_Cheswick_secure_gateway

Reference Books

- Cheswick and Bellovin, Firewalls and Internet Security, Addison-Wesley, 1994 (ISBN 0-201-63357-4)
- Garfinkel and Spafford, Practical UNIX Security, O'Reilly & Associates, 1991 (ISBN 0-937175-72-2)