Remote Administration Solutions

Console access

- Target devices include: routers, switches, load balancers, some UPSes, firewalls, and servers
- Aggregate console connections into a terminal server
- Can use a hardware terminal server with a serial or network interface to a PC that maintains access
- Alternatively, many newer terminal servers support direct network connections via SSH, with RADIUS support and IP filtering
- Can also connect out-of-band via dial-up modem with callback feature

Remote Administration Solutions

Console access

- Advantages:
  - Console messages can be logged to a terminal server
  - Central point of authentication into console management
  - Provides the ability to turn off telnet and other administrative clear-text protocols on network equipment
  - If ssh or other interactive interface fails to respond, administrator can directly connect to console without physically going to the DMZ

Remote Administration Solutions

Console access

- Disadvantages:
  - The unintentional <BREAK> problem
  - Additional hardware and cabling
  - Authentication and logging for console use (once the user has accessed the terminal server) is difficult to implement with a hardware device

Remote Administration Solutions

SSH bastion gateway

- One (hardened) point of entry via SSH to other hosts
- Can use ssh-agent to eliminate interactivity on the gateway, while maintaining only a single host that can SSH to the endpoints
- Use RSA identity files
- Disable password authentication
- Disable rhosts authentication and root login
- Bind ssh only to admin LAN interface
- Watch your patch levels – ssh is a popular target

Remote Administration Solutions

Windows GUI – 2 popular options:

- PCAnywhere
- Windows Terminal Services

Remote Administration Solutions

Windows GUI – PCAnywhere

- Risks
  - Runs on well-known port – juicy target for attackers
  - Previous versions have been vulnerable to DoS attacks and weak password encryption
  - Typical configuration binds to all interfaces
  - Should avoid exposing on an untrusted network segment
  - Typical configuration bypasses Windows login mechanism

Remote Administration Solutions

Windows GUI – PCAnywhere

- Securing PCAnywhere
  - Make use of the allowed IP addresses feature – limit admin hosts
  - Enable TCPIPHostBindMode to only listen on admin interface
  - Change default port
  - Make sure the Windows NT user is logged off after session disconnect (normal and abnormal)
  - Enable event logging and session recording (if disk space permits)
  - Utilize Symmetric encryption / Deny lower-level
  - If possible, use X.509 for host authentication
  - Disable response to PCAnywhere query broadcasts
  - Configure clients to only use TCP to connect (rather than a UDP query – reduces firewall ruleset)
  - Use separate user account for each admin with strong passwords
  - Limit login attempts
  - Only use PCAnywhere user with PCAnywhere privileges

Remote Administration Solutions

Windows GUI – Terminal Services

- Risks
  - Utilizes Windows authentication method
  - Runs on a well-known port
  - Should avoid exposing on an untrusted network segment

Remote Administration Solutions

Windows GUI – Terminal Services

- Securing WTS (for administration use)
  - Bind only to the administrative segment interface
  - Force all configuration parameters at the server level
  - Use a separate WTS login from Windows login and give each administrator unique login with strong password
  - Take Administrators group out of connection permissions
  - Enable security auditing
  - Remove TsInternetUser account
  - Utilize High Encryption for RDP
  - Disconnect idle/broken connections aggressively
  - For those who are paranoid, change the WTS port.

Logging solutions

Log types

Type	Mode
Syslog – UNIX and Network Devices	**Write to local filesystem or send over network (UDP 514)**
Windows NT/2000 Event Logs	**Write to local filesystem (network support for syslog available from 3rd parties)**
Application / Service Log Files	**Syslog, NT Event Log, flat file, binary file, database entry**

The system management need is to centralize logs for analysis.

Logging solutions

Network syslog

- If possible, limit which machines can send log entries to a host.
- Heartbeat creation and detection is absolutely imperative.
- Flood detection is also imperative.
- Syslog servers should sit on administrative LANs if at all possible.
- Make sure that clients are sending the messages over the administrative LAN interface.
- Initiatives are out there for secure syslog – not close to implementation yet:
  - Log signing
  - Encrypted transfer
  - Insertion / deletion attacks
- Take a look at syslog-ng. http://www.balabit.hu

Logging solutions

NT/2000 Event Log

- Need to get those logs off each server posthaste.
- Two major options:
  - Agent-based forwarding
    - Syslog
    - Commercial solutions
  - Batch retrieval
    - Can use common resource kit utilities to pull logs out in binary and text format
    - To push or to pull?
    - If log is cleared by an intruder, you better know about it! (Use a perl script to check for Event ID 517.)
- See my SANS NetSec 2000 presentation for many more details!

Logging solutions

Flat file logs

- Can always “syslog” them
  - tail -f /var/log/mylog | logger
  - Ok… maybe not! ☺

- Need to get them off of the originator as soon as possible.
- If they are too big and/or cumbersome, consider culling them during the push or pull process.
- How often to push/pull? Determine the criticality of the logs and analyze the worst case scenario: where the attacker blows away the local copy of the log file and your mission is to figure out what happened.
- When log disappears, you better know about it!

General tips

Watch out for administrative interfaces.

Follow best practices, especially in regards to:

- Resource utilization
- Segmentation
- Authentication
- Integrity