SAN Vulnerabilities

Charles Edge

Partner :: Three18

Author :: Mac Tiger Server Little Black Book

Fiber Channel

- Serial computer bus that is designed in much the same way as SCSI
- Can use copper or fiber optic cables
- Switches allow all devices to have equal opportunity of access
- Each devices has a WWNN, which acts like a MAC address

SAN Basics

- A SAN provides often virtualized data to client systems
- Clients often consist of servers or workstations
- Speed and massive amounts (up to a Petabyte) of space make up the predominant reasons to purchase a SAN

xSAN Basics

- Multiple LUNs are added into Storage Pools
- Multiple Storage Pools are combined to create a volume that is mounted on the client system (Apple, Windows, *nix)
- All client/server systems need access to all LUNs that make up a volume

How it Works

- Metadata, like a file allocation table, is stored on the first LUN
- Files are broken into chunks and the Metadata Controller determines which LUN each chunk will be written to
- Independent LUNs will have unreadable data

The weakness

- In order to provide equal opportunity access to the SAN each client has to have access to the metadata volume
- If the metadata volume becomes full the SAN will no longer function
- If metadata is destroyed then the SAN will no longer function

DoS the SAN

- Each LUN is shown as a disk in /Volumes
- Mount the first disk and write data to it
- Loop your write
- Wait for the SAN to crash
- Once the SAN has crashed the configuration files will be out of sync with the contents of the SAN and the volume will not restart even if the data is removed

Protection

- Close controls over physical access to the Fiber Channel switch
- Use policies to remove the access to a terminal emulator on the client systems
- Use larger LUNs to house metadata
- Maintain good backups of the metadata
- Maintain backups of your config files

LUN Masking

- Control access to LUNs based on which port a host is plugged into on the switch
- Performed at the switch level
- Swap ports and you get access to the LUNs you previously had no access to

Misc.

- If any node on the SAN is compromised typically all nodes are compromised as they all share the same data set
- LUN Masking is not a good enough security mechanism
- About 80% of fiber channel switches have the default administrative password

Demonstration

- iBook using USB Flash Drives as LUNs
- Running Xsan 1.3 with only the one system as the MDC/Client