
# Mac OS 10.3 Server Security

Charles Edge krypted

Senior Systems Engineer

Three18 - www.three18.com

# What is OSX Server?

- Mac OSX Server is a collection of Open-Source applications running on top of a Mach Kernel, with the pretty iTunes interface.
- Basically a cute & easy BSD implementation
- Any time one runs such a large number of services on one machine, security holes are bound to exist in at least one of the implementations (like BackOffice but prettier).
- At least OSX Server is better than ASIP, although a bit less secure.

# Packages in OS 10.3 Server

- Samba 3/CIFS
- Apache (1.3 and 2.0)
- LDAP
- Squirrelmail, Mailman, Postfix, Cyrus
- DHCP
- DNS
- NAT and Firewall
- MySQL
- Open Directory 2
- WebDAV, Apache Axis, WebObjects,
- VPN
- Firewall
- Tomkat
- jBoss
- QuickTime Streaming Server
- NFS
- Apple Filing Protocol 3.1
- FTPd
- Print Server (CUPS)
- Mailman 2.1.2
- PERL 5.8.1, PHP 4.3 and Ruby

# Packages added to Tiger

- Spam Assassin
- Point to Point Cabalities for VPN
- Proxy
- iChat Server
- Weblog Server
- Software Update Server
- Mac Roaming Profiles
- Certificate Management Server

# Non-Standard BSD Stuff

- MacOSXServer.conf file overrides many of the settings in standard config files for packages
- SSL needs to be done from the GUI
- AFP (port 548) is more common that SMB
- Rendezvous
- Open Directory (easy to use LDAP, but the ease of use has drawbacks…)

# Out of the Box

- Services that are on:
  - SLP
  - SSH
- Services that are off:
  - Firewall
  - WWW
  - Mail
  - FTP

# Ports to scan to ID OSX

- 548
- QTSS - 554 and 448 are common but it can be dynamic
- Open Directory

# Challenges

- Mac users aren't used to being vulnerable to security threats
- Mac users like things to be easy.  With any security improvement, things are usually more difficult (ie-implementing a vpn to replace tapping straight into the server for AFP)
- Mac users shy from modern password policies
- OSX is young and not a popular target, but if it gains market share then this will change

# Starters

- Port Scan your own block of Ips
- Brute force your own passwords

# Kerberos

- Apple is putting all their eggs in the Kerberos basket and pushing for Single Sign On using KDC
- Can also use Shadow Passwords, Passwords located in an open directory database
- Can use non-Apple servers for “simple” LDAP bind authentication

# LDAPv3

- Allows OSX to bind to Active Directory (must extend the AD Schema to obtain UID's etc.). This gives interoperability with Win2K or Win2k3 environments to OSX Server.
- Allows Apple to use Kerberos to supply "Single-Signon" access to servers.
- Allows Apple to get away from Keychains for "Enterprise Security"

# VPN Security

- Can use PPTP or L2TP/IPSec.
- Uses MS-CHAPv2 for authentication.
- Can use other methods (ie - RSA) by editing the configuration file.
- Configuration file located at: /Library/Preferences/SystemConfiguration/com.apple.RemoteAccessServers.plist
- Use VPN's to limit access between clustered machines.

# Physical Security

- The Key for Xserve's is just a pretty alan wrench.
- Lock the server down (why do we have to keep telling people this). Make sure the location has limited access.
- Use a plate to cover Xserve Drive trays (they're to easy to bump and knock off line and/or just steal).
- Enable a boot password.
- Don't put an Airport card in your server…

# Permission Based Security

- Make public folders Read Only
- Share folders, not volumes
- Enable Shadow Passwords and put spaces in them
- Limit number of concurrent CGI scripts
- Don’t enable uploading of files in Tomkat without scripting custom permissions for uploaded files



# Misc. Security Tips

- Disable unused Network adapters
- Turn off HTML tags in dynamic content
- Don’t download software from the server
- Disable SNMP on Airports
- Run regular virus scans
- Don’t set up auto-fill in your browsers
- To select services manually, go to /etc/xinetd.d or /etc/inetd.conf or /System/Library/Startupitems or /etc/hostconfig

# Account based Security

- Limit Admin accounts.  Check /etc/sudoers to mitigate access for accounts.  Sudo exists for a reason…
- Disable anonymous FTP accounts
- Use FileVault on admin accounts
- Restrict executable permission on nidump and niutil
- Restrict System Folder permissions if running Classic (like for an older LASSO implementation)



# Host Based TCP Security

- Use TCP Wrappers to restrict access
- In xinetd use the only_from and no_access to restrict access
- Look at /etc/hosts.allow and /etc/hosts.deny for more on TCP Wrappers
- Don’t change your IP once you’ve installed



# Port Based Security

- Use Firewall to block unused ports (doesn't everyone)
- Use Custom ports for services such as AFP, SMB and FTP
- Let firewalls that can protect against DoS attacks do that, 'cause OSX doesn't
- Block LDAP at Perimeter

# Manually Upgrading Packages

- Apple can be a little slower to adopt the latest patches
- Manually running patches can be risky because Software Update can replace your updates and custom files with “newer” files
- Installing upgrades can also lead to incompatibilities with the GUI
- Manually upgrading can also effect the reliability of the NetInfo Database

# Unresolved Exploits

- SSH vulnerability - Although Apple has resolved most of the issues here, some persist.  I would strongly suggest requiring VPN access to the server and then giving out SSH access only to users that require it.
- Many WebDAV apps require Public to have full access
- Stay Away from Multi-Cast DNS

# Proven Attacks - NEW

sudo find /var/Communigate -name account.settings | xargs grep Password

- Although Communigate is a 3rd party app, we've found that variations of this command can be used on other apps within OSX Server.
- One way to check for this is to grep for passwords that you know for various apps. Most apps now use NetInfo.
- Enable any laptop as a DHCP server by turning on Apple's ICS implementation

# Proven Attacks

- Apache - Use the Rendezvous binding to bypass WebDAV Realm security
- www (WebDAV) - New attack I've been working on to use any old user name and password and changing the port to trigger SSH access
- iCal password bypass
- Use LDAP to obtain full password lists

# Proven Attacks - By Krypted

- Protecting against DoS attacks - Most OSX Servers aren't protected
- NFS Man in the Middle Attack - Even though NFS is an option, figure something else out…
- If you do use NFS, MAKE SURE to restrict access to specific IP's and follow that up with MAC addresses - although both can be spoofed

# Greetings

- Use the logon greetings to send general use and policies messages for the network to users
- This helps with liability and legality issues
- Also, edit the Mac Logon screen to add general use policies



# 3rd Party Appz

- Rumpus - FTP/Web Realm Software with its own built-in Security Parameters - Once again stored in ClearText
- Retrospect - Backup Software
- Communigate - Mail/ListServ app with its own built-in Security
- Now - Like Exchange, but less secure
- FileMaker with LASSO
- Crypto-Server X
- Firewalk X

# Free Applications

- Spam Assassin/Vipul's Razor - Now Included
- BatChmod
- BrickHouse - GUI for ipfw - not needed any more
- Carbon Copy Cloner
- Preferential Treatment
- TripWire, Snort, HenWen, and Port Sentry

# Theoretically Possible

- Hacking the Network Time Service with a Man In the Middle attack
- Other WebDAV hacks
- DHCP attacks (like on early implementations of Active Directory)
- Basically, anything people thought of to do to BackOffice will probably be possible in some way to do to OSX Server, just a little later in the game…

# Thanks

- PDF's are located on the CD for Apple's manuals on different server services.
- If you don't have that, email me at cedge@three18.com for a copy.