

Mac OS X Security Tools



Three18, Inc.
2665 MAIN STREET :: SUITE 200
SANTA MONICA, CA 90405
310 581 9500 voice
310 581 9515 fax

three18.com





Three18, Inc.
2665 MAIN STREET :: SUITE 200
SANTA MONICA, CA 90405
310 581 9500 voice
310 581 9515 fax

three18.com

Three18 is a Comprehensive Technology Solutions Provider

- Apple Certified Partner
- Microsoft Gold Partner
- Symantec Security Solutions Partner
- Novell and RedHat Certified Partner
- EMC Dantz Retrospect Partner

Three18 is a Trusted Information Technology Partner to hundreds of Companies in Southern California



The talk...

- Everything we discuss should be considered as ways to mitigate attacks
- We still suggest maintaining the assumption that all systems are still vulnerable if they're online

Bastille

- As Jay talked about in his talk, Bastille is a great tool for use in locking down Mac OS X
- Most of what Bastille does involves internals and IPFW
- Through this talk we're going to pick up both from the talk I gave at DefCon a few years ago and where Jay leaves off
- This talk focuses on security from a networked services

Nagios

- Nagios
- Demo

Radmind

- Radmind
- Demo

Tripwire

- Tripwire
- CLI vs. GUI tools
- Checkmate Demo

Snort

- libpcap
- Snort
- HenWen
- Letterstick
- Guardian
- DoS vulnerability with IPS
- Demo

Apple Remote Desktop

- ARD
- Keeping Software updated
- Sending shell commands to clients
- Demo

Open Directory Password Policies

- GPO tools in Active Directory helped to make Windows systems on a large scale more secure
- Open Directory applies mcx policies which help to perform the same task
- Demo

IPFW and beyond

- IPFW has many rules both from the incoming and outgoing ways
- Dummynet provides a way for administrators to shape traffic as it's coming into ipfw
- This expands traffic control from a typical allow/deny and into a more flexible manner that allows administrators to specify a limit for maximum bandwidth

Centrify DirectControl

- Centrify DirectControl provides Mac administrators the ability to configure policies for groups of Mac users using the Active Directory Users and Computers snap-in
- Using DirectControl allows administrators to control policies for Mac users without having to establish what is known as the Golden Triangle, a method for building a cross-realm so you can provide user credentials using Active Directory and policies using Open Directory

Dave and AdMitMac

- Thursby
- Dave
- Demo

- AdMitMac
- Demo

Reacting to Security Incidents

- Securing a system is one thing, but making the assumption that something is going to happen at some point is also an important part of security
- Network administrators should have a clear plan for what they will do when something happens
- Servers should often have tools loaded on them and ready to use
- Writing a shell script that will run a snapshot and dump log files to checksummed files is a great tool, much like the Symantec iButton

Building Your Own Tools

- If there are no tools for performing a certain function you can always build your own
- We have done this for clients using a combination of shell scripts, perl and anything else we happen to dig out of our toolbox
- Once you build a tool, you can easily add a Cocoa wrapper to it
- Once you have a tool built, you can continually update it or add it to the Open Source community and allow the tool to often take a mind of its own

Mac OS X Security Tools



Three18, Inc.
2665 MAIN STREET :: SUITE 200
SANTA MONICA, CA 90405
310 581 9500 voice
310 581 9515 fax

three18.com

