

10 Ways to Not Get Caught Hacking On Your Mac



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...

- First, I'm not condoning doing anything that requires you to need to hide anything!
- The more collaborative the better.
- But, let's get through the talk first due to time constraints.

#1 - Time Stamps

- Time stamps help establish a timeline of forensic tracking. This extends from time modified to time created as well.
- While changing the time stamps of every file on your operating system isn't a cure-all, it does make establishing a timeline more difficult.
- You can run a shell script that will touch every single file on your operating system nightly
- This will effectively make tracing the last modified dates impossible (but don't forget about those creation dates)

#2 - No History, No Trace

- The history keeps a listing of all the shell commands run on the system
- Many GUI tools actually run shell commands and log their run commands into the shell history
- Clear the history files on the system
- This helps to make sure that the most recently run commands will not be able to be found

#3 - Keep the Trash Empty and Do So Securely

- Just throwing a file away doesn't get rid of it
- Emptying the Trash does little better
- Secure Empty Trash really, really gets rid of files
- You can cron Secure Empty Trash by using the srm command, which is the open source utility that the feature is built on top of
- When you use the srm command, use the -f flag to force emptying
- Use the -m to overwrite the data with 7 passes of random data and zeroes

#4 - Don't Keep Firewall Logs

- If you're the type of person that clears out the firewall logs of remote systems then you should likely be clearing out your own firewall logs as well
- ipfwloggerd will log firewall activity on your system
- This can be disabled and it won't log data any more
- Still delete those logs at /private/var/log/ipfw.log
- Oh, and the archives at /private/var/ipfw.log.*.gz

#5 - Use FileVault

- FileVault encrypts your home folder into a dmg file that is encrypted with AES encryption
- If someone wants to get into your filevault they will be able to but this will slow things down
- If you use a very complex password then it will be more difficult to decrypt that filevault password
- The Master Password can unlock any filevault disk images, so make sure that this password is uncrackable

#6 - Use Encrypted Disk Images for Everything

- Like with filevault, encrypted disk images store data in encrypted files
- These are easy to create and provide an additional level of security, creating an encrypted disk images inside of encrypted disk images
- If you don't use encrypted disk images you can use secure channels. For example:
 - Metadata in music files in iTunes library in the filevault
 - Hidden image data in an iPhoto library in the filevault
 - Hidden data in comments field of Word documents in an encrypted disk image the filevault

#7 - Clear those logs

- Log files help to establish the actions that were taken, the systems that you have connected to and what was done on those systems
- Remember when running a secure shell that there are two sets of logs to clear
- Most logs are stored in `/private/var/log/`
- Console can be used to view where the others are stored and you have a nifty clear button to clear specified logs

#8 - Secure Virtual Memory

- Virtual memory is a place that forensics specialists often look to reconstruct the last moments before a system was restarted
- By using the secure virtual memory feature you will make it where it is not possible to access the previous virtual memory of a system following its restart

#9 - RAID

- Concatenated RAIDs are JBODs
- A JBOD can easily be reconstructed with a missing member, but it provides one more layer of security
- This is nice for boot volumes where you are required to use a jump drive to boot the system
- If you use Xsan to stripe two USB jump drives then you will be able to control the stripe methods that is used to write data to your mini-SAN
- By storing only half the data on each drive you mitigate the ability that the data will be reconstructed

#10 - Just Don't Keep Stuff

- You can't get in trouble if you don't have data
- Physically destroy the system disks and RAM
- Don't keep data on your system doesn't mean you don't have to keep data at all
- Secure channels on untraceable remote systems is always another way to store data
- If you don't compromise a system too far then people will often never notice data on the system
- Most people (especially in small businesses) will just delete a file rather than try and trace it

10 Ways to Not Get Caught Hacking On Your Mac



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

three18.com

