Privacy & Security Lab

Hoofnagle / Info 290 005

Lab 2, February 7, 2017

**Web Tracking and Cookies**

Important: While we are in the lab, please do not access any sensitive information. Do not check your personal email, login to IM, and so on. By taking part in this exercise, you consent to monitoring and you are aware you will be monitored. Do not use any of these techniques for evil (I know it when I see it!), today or later. Do not surf for offensive or illegal content.

The login and passwords for all the iMacs are the same:

login: XXX

password: XXX

The login/password for Kali is

root/toor

1. Please login, open VirtualBox, and start your Kali image.
2. The basics of tracking
	1. Find your computer’s IP address by opening the Terminal and typing **ifconfig** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
	2. What else does ifconfig report?
	3. Now, using Firefox within Kali, visit ipchicken.com and compare the reported IP address \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
	4. The active network hardware (Ethernet, wifi, Bluetooth, etc) in your computer have globally-unique identifiers (GUID) that are reported when you use the command **ifconfig**. To see all of the computer’s device identifiers, try
	**hcitool scan** (for Bluetooth components) and **ip link show** (**ifconfig –a** should also work)
		1. Fyi, on a Mac you can do this with **networksetup –listallhardwareports**
		2. Fyi, on a PC, you would use **ipconfig** or **netstat –a**.
3. Data Everywhere
	1. Use the command traceroute to see how information from your computer originates from your IP address and traverses the internet, e.g.
	**traceroute yahoo.com** or **traceroute yandex.com**
	2. You’ll see that traceroute shows us a little bit about Berkeley’s network setup. Your computer is connecting to a gateway (probably something like 10.0.0.1) and then presented to the public network through a Berkeley-held IP address (something like 128.32.226.xxx).
	3. The website <http://www.monitis.com/traceroute/> has a visual trace route tool that links location to each of those IP addresses. Try a few traces using Firefox in Kali and see if you can get a request for a website routed outside the United States. If your request crosses a national border, most nations believe that it can be monitored without any criminal predicate. Thus, where one puts their servers, or has their traffic routed, can have profound consequences for privacy.
4. Configure Firefox in Kali

Figure 1 Those three solid lines on the upper right hand side represent the "hamburger"

* 1. Start Firefox in Kali
	2. Click on the “hamburger”
	3. Click on preferences
	4. Click on privacy
	5. Now, do you see anything about cookies? How would you block cookies in Firefox?
	6. Try manipulating the settings in this tab to see what happens.
	7. Before you finish this task, be sure to set Firefox back to “remember history”
1. Comptrast Chrome
	1. For this comparison, use the Mac OS (Kali does not have Chrome, so just use the desktop computer’s installation of Chrome. Keep Kali running in the background).
	2. Try finding the privacy settings in Chrome. Start by clicking on “Chrome > preferences” or simply press ⌘,(command and comma)
	3. What are the default settings? Are they the same as Firefox?
	4. How does the Chrome privacy language compare to Firefox?
2. Online Profiling
	1. Visit the Oracle Data Cloud Registry (http://www.bluekai.com/registry/) using Chrome in the MacOS environment
	2. What does the site claim it has observed about browsing activities?
		1. Now go visit some sites of interest (remembering our no sensitive, no offensive sites rule)
		2. Periodically return to the Oracle site to see whether these visits influence the profile.
	3. Now switch to Firefox within Kali and repeat this exercise.
	4. Are there differences?
3. Very Basic Device Forensics
	1. Trade terminals with a classmate.
	2. Inspect the cookies on the computer
		1. For Firefox, go to Firefox > Preferences > Privacy > Show Cookies or remove individual cookies
		2. For Chrome, go to Chrome > Preferences > Settings > Show advanced settings > Content settings > All Cookie and site data
	3. Recall from last week that we learned about a dozen different tracking techniques. Can you find other evidence of what sites were visited by your classmate?
4. Basic Photos Forensics
	1. Find a high-quality photo online (such as a portrait) and submit it to <http://exif.regex.info/exif.cgi>
	2. The service extracts metadata from photos. You’ll see that if you choose a high-quality photo, the kind that comes from a DSLR (a fancy camera), there is a yuge amount of information about the image, including whether it has been edited, when it was taken, and so on.
	3. Some cameras encode their serial number to .jpg files. And so, you can use a service like this one to see whether other pictures are on the web taken with the same camera: <http://www.stolencamerafinder.com/>
5. Logging
	1. I’ve set up a site for the class on EC2. Visit it here: http://XXX/
	2. Login to our instance using the Kali Terminal emulator with this command:
		1. **ssh -l [USERNAME]** **[IPADDRESS]**
			1. By entering that command (ssh, for secure shell client, you start an encrypted communication from your computer into the remote server, XXX using the username “XXX”)
		2. The password is **XXXX**
		3. Position your Terminal and Browser such that you can see both at the same time
		4. In Terminal, type **cd /var/log/httpd**
		5. Type **ls**
		6. Recall that one can view text files with several commands, including **cat**. Because we are looking at live logs (these are in the file access\_log) that are updating as we visit our server, it’s best to use **tail –f access\_log**
		7. When you want to exit tail, press **control-z**
		8. Go back to the browser and reload the site: http://XXX/
		9. See if you can make sense of the information in the access log.
	3. See what else you can find on our class website.