Cybersecurity Across Curricula!
Digital Forensics - Mini-Lab

University of Hawaii Maui College

Debasis Bhattacharya

Fall 2019

Table of Contents

Expected Duration

~1 hr, 15 min
ExifTool demo - 20 minutes
Ping and Traceroute lab - 5 to 10 minutes
Password security - 20 minutes
Wayback machine - 5 to 10 minutes
Cellphones - 5 to 10 minutes

Prerequisite Knowledge

- Command-line interfaces (directory navigation, etc.)

EXIF Data

- Information on EXIF - https://exifinfo.org/
- Online EXIF Viewer - https://www.verexif.com/en/ and http://exif.regex.info/exif.cgi

Ping and Traceroute lab

Context: Ping and Traceroute are important system tools that should be learned before diving into Wireshark or other network based tools. They enable you to find out more about a network for reconnaissance.

Requirements:

- Any computer

Procedure:

Traceroute - This is a network tool that lists the hosts that your computer has to hop through in order to get to your destination. The internet is not as simple as just connecting directly to a

server, but rather, you hop different networks in order to reach that server. This tool is called tracert on Windows, while it is called traceroute on Linux/OSX

On a command line type in “[tracert/traceroute] www.bbc.net.uk”

- bbc.net.uk is in the United Kingdom, so we will see the servers/routers your computer goes through to get there.
- You’ll notice a drastic jump in time (measured in milliseconds) in between hops, you can assume that’s the time it took for the packets to move across the pacific/atlantic ocean.
- There are three columns showing different times, this is because traceroute sends three packets by default, so normally you would take the average of the three times.

Ping - This is a network tool used for testing whether or not a computer is online (locally or globally) It sends an ICMP packet that makes a round trip. If the packet is not returned, then the computer might be down or blocking ping packets. This tool also measures latency, or the amount of time taken for the packet to make a round trip.

- ping www.google.com
- ping 127.0.0.1
  - This is the localhost, so latency 0ms.
- ping eng.kremlin.ru

- This is the website for the president of Russia, notice the latency is a lot more than google, latency often has to do with the amount of devices your connection passes through as well as geographical factors such as distance.

Password Security

1. Video - https://www.youtube.com/watch?v=MY3XWYr726I
2. https://howsecureismypassword.net
3. https://haveibeenpwned.com

Wayback machine

https://archive.org/web/

Cell phones

1. Connections / beaconing / tracking (Cell Site Location Information / Mobile Telephone Switching Office)
2. https://imei.info

Sample Quiz

Digital Forensics Quiz

1. What kind of malware is known for being disguised as legitimate software?
    a. Virus
    b. Trojan
    c. Rootkit
    d. Keylogger
    e. Worm
    f. Zero Day
2. What should you do if you encounter a running (but locked) computer at a crime scene?
    a. Unplug it immediately; it could be infected
    b. Try to guess the password: many are easy, such as 1234 or Password!
    c. Carefully shut it down to prevent data corruption
    d. Make arrangements for analysts to create forensic copies of data
3. Follow up question: what should you consider doing if it appears that a user left their account logged in?
    a. Start searching for evidence; you may have minutes to hours before it is deleted remotely
    b. Change the password so you can log back in; that way you can shut it down for transport
    c. Use it to log into your social media accounts and upload selfies of you investigating the scene
    d. Use a mouse jiggler to keep it unlocked
4. How can EXIF data be useful?

    _____
    _____
    _____
    _____
    _____
5. What is the difference between ping and traceroute?

    _____
    _____
    _____
    _____
    _____
6. Why shouldn't you use a password like SecretPassword1 or mypassword?

    _____
    _____
    _____

Quiz Answers

---

1. b. Trojan
2. d. Make arrangements for analysts to create forensic copies of data
3. d. Use a mouse jiggler to keep it unlocked
4. EXIF data may tell you many things about a photo, such as the date and time of creation, GPS coordinates where taken, and the brand and model of the camera used.
5. Ping shows the latency of communication between two computers, while traceroute does the same in addition to showing which computers the connection goes through.
6. Password cracking algorithms are sophisticated to the point that passwords which make use of dictionary words and few special characters or common ideas are easily cracked in relatively little time.
