CSE 345/545: Foundations to Computer Security

ASSIGNMENT 2

Deadline: October 30th, 2021

Instructions:

- You have to add terminal commands and screenshots of the terminal along with the answer wherever necessary.
- We will strictly check your solutions for plagiarism, ensure you do it independently.
- We will take a demo while evaluating, therefore, make sure whatever commands you write in your solutions, must work with your system.

---

1. If the stolen data is encrypted, should the organization still notify the security breach? Why or why not? Find real-life examples to support your answer.

   [5]

2. How are Anonymization and Pseudonymization different? Given the below example for Patient information, how will the data look after Anonymization and Pseudonymization:

   Patient John Doe has a gamma-GT value of 83U/L **[5]**

3. Consider the privacy policy of:
   - Any 5 social media e.g Facebook, Twitter, Instagram, and Reddit, etc.
   - Any 5 e-commerce websites: Amazon, Flipkart, Snapdeal, etc.

   a. Compare the length of the privacy policies and show a bar chart of lengths.
   b. Compare the text's complexity based on factors like sentence length and the difficulty of vocabulary.
   c. Comment on the privacy policy of the websites on the above 2 metrics and compare them among each other. **[5+5+10= 20]**

4. Metadata, information about information, is essential in forensics. ExifTool is a tool to see, update or delete metadata. It is an open-source tool that allows reading, writing, and editing metadata information in a wide variety of files. This tool can be downloaded from here. http://www.sno.phy.queensu.ca/~phil/exiftool

   a. Find the location from the metadata of the image, and report the city and country where the image is taken.
   b. As an attacker, you want to modify the location of the image and change it to IIIT-Delhi.

c. Find the md5 checksum of the image before performing b. And after b. Are they the same? Explain your answer.
d. Can we trust the file extension of a file for forensic purposes? Change the extension of the image provided to something else. What changes do you observe in the data/metadata of the file?

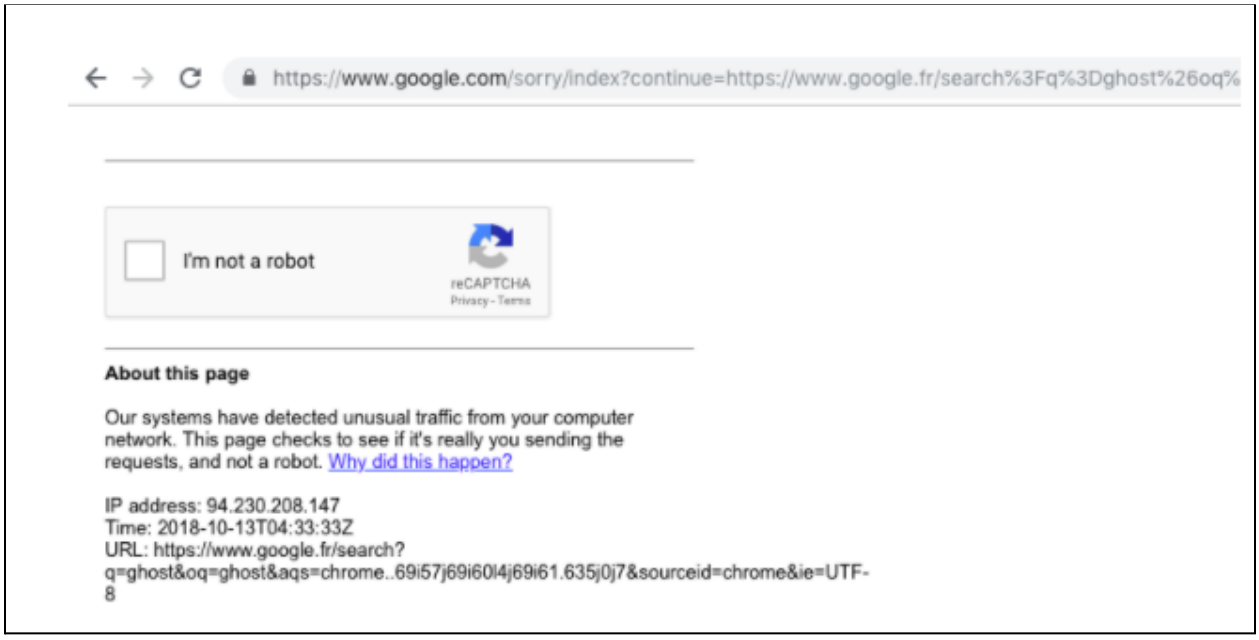
You have to add commands and screenshots of the terminal with the answer.

[2+2+3+3=10]

5. While using a system like Tor, we must route our DNS traffic through the system to ensure privacy. Why? **[3]**

6. You have to install Tor without Tor Browser and configure it to be used with any browser on your system. Show all the commands you will use and screenshots of the terminal wherever necessary. **[7]**

   Hint: When your Tor service is running successfully, you will see something like this:



   Also, report the auto-generated hostname generated by Tor.

7. Use OpenSSL(https://www.openssl.org/docs/manmaster/man1/enc.html) to answer the following:
   a. Generate a public key for your system, and configure the VM assigned to you for password-less authentication.

b. Which of the ways: with the password, or with the public key, do you think is safer?
c. Generate three different text files having 100 lines of text, 100k lines of text, and 100M lines of text. Encrypt each of the files using RC4, AES-256, and RSA using the key generated in step a.

Share screenshots and commands wherever necessary. **[4+2+4=10]**

8. Nix-based systems have an embedded industry-standard firewall called a packet filter. It uses the net-filter framework inside the Linux Kernel and BPF (Berkely Packet Filter) subsystem in BSD-based systems. The Linux variant of packet-filter is iptables. A replacement of iptables called nftables is also under heavy development. Use iptables to:

   a. Disable Echo-Reply (ping) to your machine. Your machine should not reply to ping from any other machine (act dead/not available). You should be able to ping other devices though. **[2+2=4]**
   b. Host a webpage on your machine. Use iptables to only allow your own mobile-phone to access the web-page and block all others. **[2+2=4]**

9. WebGoat is a deliberately insecure application that allows interested developers to test vulnerabilities commonly found in web-based applications that use common and popular open-source components. You can use docker to run Webgoat: https://github.com/WebGoat/WebGoat.

   There are 32 short lessons that explain web application vulnerabilities and attacks. You will get a mark for completing each lesson. **[1x32=32]**

   Share screenshots of each completion and your observations.

   [Bonus Marks] You will get bonus points for solving challenges present in WebGoat. **[4 for each]**