**CPSC 4200/6200 Fall 2021 Homework 2 50 points**

**Name: Rajat Sethi and Sai Krishna Musunuri**

This homework is done *individually,* or in teams of 2. (No more than 2)

You are allowed to use search engines, textbook/s, lecture notes, and any other sources you wish. But you are *not* allowed to copy paste from Internet, or help others with their work, either by giving out hints or solutions.

You will take a number of screenshots. All screenshots should be clearly legible and illustrate without a doubt what you are doing. You can open them in an image editor of your choice and trim off the parts you do not need, just to make images smaller. Insert them when answering the question, *do not* submit them separately as image files. Since this is an *editable document,* you can make space between the questions and type your answers and insert your screenshots here. Please do not type in red, any other color is fine. I read everything you write, so if you just type in black, I will not miss your answer 😊

**What and how to submit**

Save your assignment as pdf file with both of the teammates’ names on it. Submit to canvas. You will have an additional 24 hours to submit your assignment with 10 point late penalty. As soon as *Assignment 2* link closes on canvas, *Assignment 2 Late* link will open. When this link is closed, no late assignments will be accepted. Please do not e-mail your assignments.

**Grading and Points**

Every question indicates how many points it is worth. 4000-level and 6000-level are graded differently, with points indicated as (x/y), where x is 4200 and y is 6200.

**Exercises**

1. In this exercise you will experiment with an open source packet analyzer Wireshark (formerly known as Etherial). Download/install Wireshark and look for a tutorial online. When you are done with the tutorial, experiment with Wireshark and show how someone with malicious intent could use it to obtain useful information. What useful information could they obtain using Wireshark? Is there a way to prevent this? Include 4-5 screenshots to illustrate your points. Screenshots should be legible ( you can trim them in an image editor) and clearly illustrate the points you are making. (20/18)

Wireshark is a packet sniffing tool used to intercept networking packets on a connection. This application is normally used to analyze network traffic and request/response data. A user chooses the connection they want to examine, and the application pulls the packet data into a large list which can be filtered.

Graphical user interface, application, Word

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

One of the main malicious ways to use Wireshark is by sniffing Telnet packets. Telnet is a network protocol like SSH that is used to communicate with a remote server. The main difference being Telnet sends unencrypted data. If a malicious individual were on a public connection (like an ethernet LAN), then they could steal private data depending on the terminal commands sent. This includes login forms, document text, or even banking information.

Table

Description automatically generated

In this example, I created an account on a test server using Telnet. Wireshark was able to capture my username and password cpsc6200, one packet at a time (they were the same for this example, I only have the username shown because it would have been repetitive).

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application, Word

Description automatically generated

Graphical user interface, text, application, Word

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application, Word

Description automatically generated

Graphical user interface, text, application

Description automatically generated  
In addition, I was also able to sniff the results from running linux commands. In the example below, I have screenshots of the output for the “help” command. In a more sinister attack, the information from files could be siphoned, especially with the “cat” or “less” commands.

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Text

Description automatically generated

1. Investigate three different websites of your choice (except amazon.com, google.com and clemson.edu) in terms of their authentication requirements: what is the length of the passwords that they require? What are password rules on that site? Are reused passwords allowed? Do they use account lockout? For how long? How often do users have to change these passwords? If a user forgot the password, what is the password reset procedure? Does the website use CAPTCHA? Please answer all of these questions and include 1 screenshot for each site. Questions/answers can be organized as a table. As a conclusion to this exercise, please state which of the three websites has the strongest password security, and explain why it is so. (10/8)

|  |  |  |  |
| --- | --- | --- | --- |
|  | CNN.com | Chess.com | Github.com |
| Username Requirements | Use E-Mail Address | Must be Unique  Must be Alphanumeric  E-Mail Also Required | Must be Unique  Must be Alphanumeric  E-Mail Also Required |
| Password Length | 12+ Characters | 6+ Characters | 15+ Characters OR (8+ Characters WITH 1+ Number) |
| Capital Letters? | Not Required | No | No |
| Numbers? | 1+ Numbers | No | 1+ Number, if <15 characters. |
| Special Characters? | 1+ Special Characters | No | No |
| Repeated Characters? | Allowed | Allowed | Allowed |
| 2FA? | No | No | Optional |
| Password must be Unique? | No | No | See Other\* |
| Account Lockout? | No | Yes, after 10 tries it locks out for 10 minutes. | Yes, after several log-in attempts, there is a rate limit up to 1 hour. |
| Forced Password Change? | No | No | No |
| Password Reset Procedure? | E-mail (30 Minutes) | Give Username & E-mail, then respond to Reset E-mail. | Give E-mail Address and solve CAPTCHA, then respond to Reset E-mail. |
| Security Questions? | No | No | No |
| CAPTCHA? | “Protected by reCAPTCHA” | Yes, when resetting password or after three failed log-in attempts. | Yes, during account creation and password reset. |
| Other? | None | None | \*Passwords cannot be used if they are susceptible to dictionary attacks.  Account Creation Requires E-Mail Verification. |

Graphical user interface, website

Description automatically generated

Graphical user interface, application, website

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface

Description automatically generated

Graphical user interface, text, application

Description automatically generated

I believe that out of the three websites I analyzed, GitHub has the best security. They have the strongest account setup requirements, password components, and use of captchas. In addition, they rate limit login attempts to prevent bot attacks if they somehow get past the captcha. If that is still not enough, other security measures can be implemented in the settings, like 2FA. Compared to CNN and Chess.com, GitHub takes its cybersecurity a lot more seriously.

1. Design a security system for a small company (description below). The map of the property is on the next page. (20/18)

A small privately owned company (*Ziemenz, Inc.)* that manufactures custom controller cards just moved into a corner lot of a quiet residential neighborhood in the suburbs of a large city. The one-story building is about 2000 sq. feet. The land lot is 1 acre, with trees on two back sides and small residential roads on two other sides (see property map on next page). The building has three entrances. There is a small shed with valuable components and materials in the back corner of the lot that has a large padlock on the rollup door. The company has 2 offices for employees with freshly installed computer system with 2 Dell Latitude laptops running a freshly installed Ubuntu Linux 20.04, and a small component assembly room where the controller cards are put together.

With civil unrest coming to large cities, the owners have a concern about their business being vandalized, burglarized, or destroyed. The two owners have hired you to design a comprehensive security system that includes both the exterior and the interior physical security. You were also asked to secure their computer system (that contains intellectual property) from possible cyberattacks. System also needs a backup plan. They also requested some smart wireless security cameras, so they can monitor the area around the building at all times, including at night.

Since the company is located in the residential neighborhood, the owners want to blend-in with the surroundings and do not want to attract attention with barb-wire fences or vicious guard dogs. They are willing to spend a reasonable amount of money to ensure their business continuity. Please develop a comprehensive proposal for the owner where you will outline all the security mechanisms that the company may benefit from (from door locks and cameras, to firewalls and IDS and backup services). Be specific and detailed while recommending certain features. For example, recommend a specific firewall product, specific camera, etc. If you do not have enough information to recommend a feature, you can make any reasonable assumptions. *Ziemenz, Inc* thanks you for your time.

*Map on next page*

**\*indicates entry**

**\***

**\***

2-lane local road

**\***

**\***

**\***

shed

building

2-lane local road

driveway

Physical Security:

* Fences
  + The perimeter should be surrounded with a regular fence. Wooden or Chain-Link will work fine.
  + The fence gate should be protected with a lock. If the company decides to use RFID Cards, then they should also apply those cards to the gate.
  + If the company decides to use a regular lock instead, then I recommend the Bowley Lock, a complex lock with extreme resistance to lock-picking.

A picture containing lock, metalware

Description automatically generated

* Surveillance System/Cameras
  + For the surveillance, I recommend using the SimpliSafe system.
  + SimpliSafe offers a multi-piece security system such as motion-detectors, cameras, panic buttons, alarms, and keypads.
  + I recommend buying seven surveillance cameras. One inside each entry point, one at the back of the building, two inside the main building, and one inside the shed.
  + As for motion detectors, there should be one at each entry point to notify the owners if anyone enters the building. This includes the shed.



* NFC Keycards
  + To secure access into the building and each of the rooms (especially the computer and finance rooms), the employees should use NFC Keycards instead of physical keys. Many physical keys are subject to non-destructive lockpicking, but NFC systems are much harder to break into without causing physical damage.
  + NFC cards support encryption as well, so they cannot be forged or copied easily.
  + NFC cards also support multi-factor authentication and pins unlike regular RFID cards.
  + The main distributor for these smart cards is HID Global. Their website and products can be found here, which can be professionally installed by their employees.
  + <https://www.hidglobal.com/products/cards-and-credentials>



Virtual Security:

* Passwords
  + All passwords on the system must be “strong” and “unique”
  + 8 alphanumeric characters+
  + At least 1 uppercase and 1 lowercase letter
  + At least 1 “special” character
  + Cannot appear in any list commonly used for dictionary attacks.
* Firewall
  + GUFW is a firewall that can be downloaded for Ubuntu systems.
  + It can control traffic and report/log any suspicious activity.
  + See the documentation at <https://help.ubuntu.com/community/Gufw>

Graphical user interface, application

Description automatically generated

* Backup Systems
  + The most reliable backup system is an anacron job set to run at certain intervals.
  + Set the job to copy and backup the most important files daily, then send them to a secure cloud system like AWS or Google Cloud.
  + Most of the system and less important files should also be backed up every one or two weeks and sent to AWS/Google Cloud.
* Logging
  + All commands, files, and applications should be logged, rotated, and monitored for suspicious activity. These logs should be stored in a file and stored on AWS/Google Cloud.

**Graduate Students:**

System administrators are often tasked with selecting and even installing the proper video surveillance system for the organization. Please do an online research and find three candidate video security systems. The cost of the system should be no more than $600 USD. The motion activated system should have recording capabilities (on an insertable card of some kind, not dvr), night vision, and being able to be accessed from a phone or an ipad for monitoring over the internet. Ease of installation should also be considered. Justify why you are recommending your selected systems. Which one is the best of the three? (0/6).

System 1: Ring Surveillance Cameras

Graphical user interface, text

Description automatically generated

At $360, Ring offers one of the best security cameras on the market. They are wireless cameras that can connect to most of your devices for monitoring and recording (i.e., PC or Tablet). In addition, these cameras have night vision and motion sensing capabilities to detect intruders and alert the owner before a break-in happens. Consumers have an easy and successful time using this product, as 1,400 reviews have given an average rating of 4.6 / 5.

System 2: Blink Surveillance Cameras

Graphical user interface, application, Word, website

Description automatically generated

At $180, Blink provides two easy-to-setup wireless cameras that can connect to your phone, tablet, and Amazon Alexa. The battery life is incredibly long and can run for up to 2 years. In addition, the cameras are very light, and so they are hard for criminals to notice that they are being recorded. With over 4700+ reviews, customers are satisfied with an average rating of 4.3.

System 3: SimpliSafe Security Package

Text

Description automatically generated

At $200, the SimpliSafe Security Package comes with a large ensemble of protective devices. First, there is the surveillance camera that sends video directly to PC/Tablet/Phone and allows recording in HD. There are also the door sensors that activate when any of the entryways are accessed. The panic button alerts authorities in the case of an emergency or break-in. The base station uses voice control to configure and monitor all the other components. The keypad can be used to turn the system on and off when necessary. Combined, these devices make for one of the most complex and powerful security systems on the market. Consumers love this product, with over 500 reviews giving an average score of 4.5/5.

Out of all three of these systems, I believe that SimpliSafe provides the most protection for its price. There are door sensors, cameras, and other monitoring devices all in one package. Unlike the other two systems, SimpliSafe does not just really on video evidence, it also uses motion detection and can alert the authorities before any damage can occur. For the low price this system is offered at, there is nothing that can really top this product in the current market.

Undergraduate students can do graduate student exercise for 5 extra credit points.

Graduate students can explore 3 firewall products for Linux for 5 extra credit points.