

Name: 1.Rajat Sethi

2.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

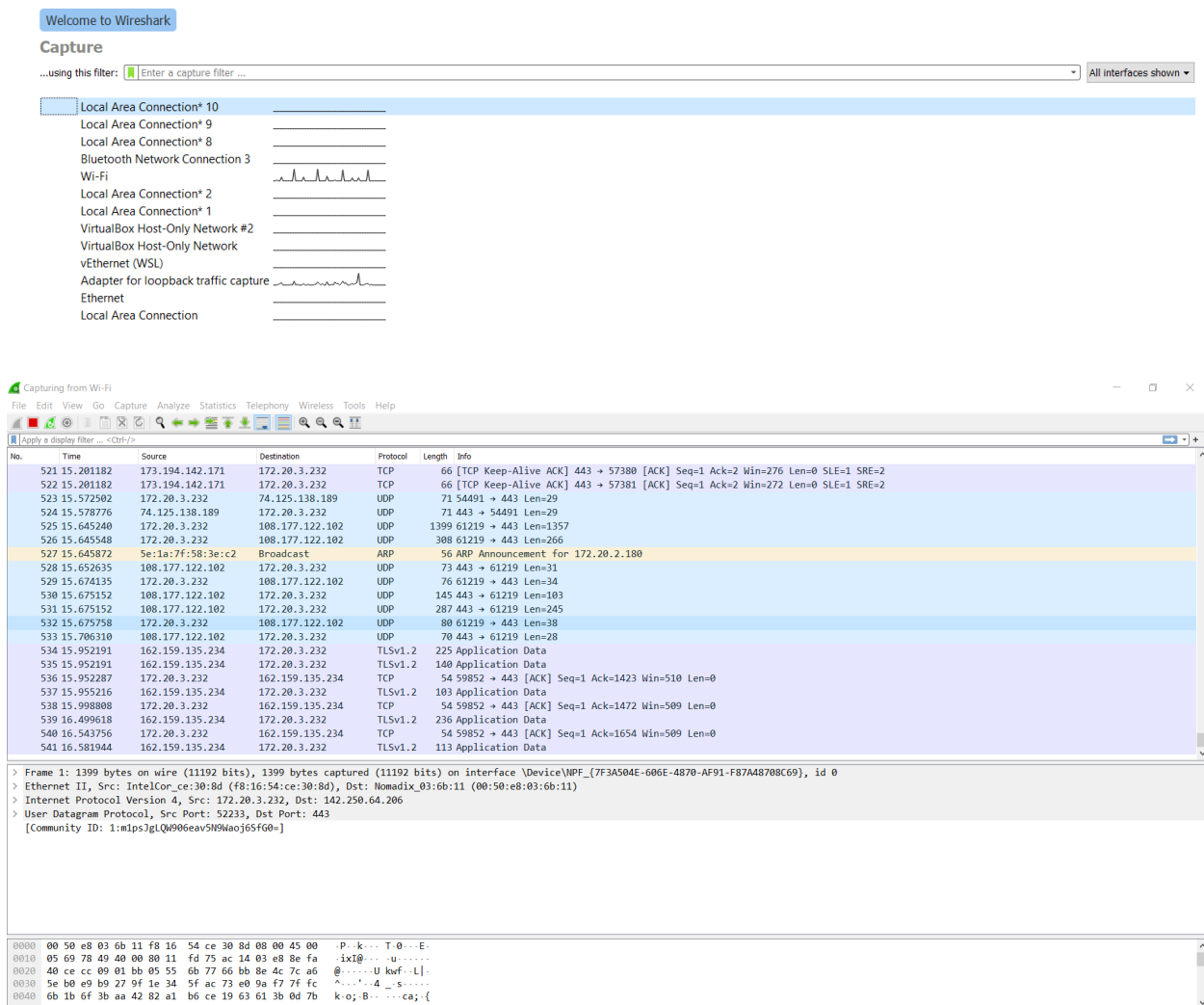
Every question indicates how many points it is worth. 4000-level and 6000-level are graded differently, with points indicated as (x/y), where x is 4200 and y is 6200.

### Exercises

1. In this exercise you will experiment with an open source packet analyzer Wireshark (formerly known as Etheral). 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.



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.

No.	Time	Source	Destination	Protocol	Length	Info
23441	709.647980	64.13.139.230	172.20.3.232	TELNET	110	Telnet Data ...
23506	716.714438	172.20.3.232	64.13.139.230	TELNET	55	Telnet Data ...
23512	716.779280	64.13.139.230	172.20.3.232	TELNET	60	Telnet Data ...
23514	716.857525	172.20.3.232	64.13.139.230	TELNET	55	Telnet Data ...
23515	716.922367	64.13.139.230	172.20.3.232	TELNET	60	Telnet Data ...
23516	716.948205	172.20.3.232	64.13.139.230	TELNET	55	Telnet Data ...
23517	717.013337	64.13.139.230	172.20.3.232	TELNET	60	Telnet Data ...
23518	717.059392	172.20.3.232	64.13.139.230	TELNET	55	Telnet Data ...
23519	717.132077	64.13.139.230	172.20.3.232	TELNET	60	Telnet Data ...
23544	718.041117	172.20.3.232	64.13.139.230	TELNET	55	Telnet Data ...
23545	718.106557	64.13.139.230	172.20.3.232	TELNET	60	Telnet Data ...
23547	718.308282	172.20.3.232	64.13.139.230	TELNET	55	Telnet Data ...
23548	718.374456	64.13.139.230	172.20.3.232	TELNET	60	Telnet Data ...
23552	718.519686	172.20.3.232	64.13.139.230	TELNET	55	Telnet Data ...
23554	718.584066	64.13.139.230	172.20.3.232	TELNET	60	Telnet Data ...
23556	718.678970	172.20.3.232	64.13.139.230	TELNET	55	Telnet Data ...
23557	718.743509	64.13.139.230	172.20.3.232	TELNET	60	Telnet Data ...
23559	719.350006	172.20.3.232	64.13.139.230	TELNET	56	Telnet Data ...
23560	719.419389	64.13.139.230	172.20.3.232	TELNET	60	Telnet Data ...
23565	719.534863	64.13.139.230	172.20.3.232	TELNET	64	Telnet Data ...
23603	721.386817	172.20.3.232	64.13.139.230	TELNET	55	Telnet Data ...

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).

> Frame 23441: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface \Device\NPF_{7F3A504E-606E-4870-AF91-F87A48708C69}, id 0
<ul style="list-style-type: none"> <li> <ul style="list-style-type: none"> <li>Ethernet II, Src: Nomadix_03:6b:11 (00:50:e8:03:6b:11), Dst: IntelCor_ce:30:8d (f8:16:54:ce:30:8d) <ul style="list-style-type: none"> <li>Destination: IntelCor_ce:30:8d (f8:16:54:ce:30:8d)</li> <li>Source: Nomadix_03:6b:11 (00:50:e8:03:6b:11)</li> <li>Type: IPv4 (0x0800)</li> </ul> </li> <li>Internet Protocol Version 4, Src: 64.13.139.230, Dst: 172.20.3.232</li> <li>Transmission Control Protocol, Src Port: 23, Dst Port: 52554, Seq: 16779, Ack: 252, Len: 56</li> <li> <ul style="list-style-type: none"> <li>Telnet <ul style="list-style-type: none"> <li>Data: ?You may not create test accounts on 'alts'.\r\n</li> <li>Data: Username:</li> </ul> </li> </ul> </li> </ul> </li> </ul>
[Community ID: 1:CnE5b/nT6cD2hmPK/PKzWb5jLU=]
> Frame 23506: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{7F3A504E-606E-4870-AF91-F87A48708C69}, id 0
<ul style="list-style-type: none"> <li> <ul style="list-style-type: none"> <li>Ethernet II, Src: IntelCor_ce:30:8d (f8:16:54:ce:30:8d), Dst: Nomadix_03:6b:11 (00:50:e8:03:6b:11) <ul style="list-style-type: none"> <li>Destination: Nomadix_03:6b:11 (00:50:e8:03:6b:11)</li> <li>Source: IntelCor_ce:30:8d (f8:16:54:ce:30:8d)</li> <li>Type: IPv4 (0x0800)</li> </ul> </li> <li>Internet Protocol Version 4, Src: 172.20.3.232, Dst: 64.13.139.230</li> <li>Transmission Control Protocol, Src Port: 52554, Dst Port: 23, Seq: 252, Ack: 16835, Len: 1</li> <li> <ul style="list-style-type: none"> <li>Telnet <ul style="list-style-type: none"> <li>Data: c</li> </ul> </li> </ul> </li> </ul> </li> </ul>
[Community ID: 1:CnE5b/nT6cD2hmPK/PKzWb5jLU=]
> Frame 23514: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{7F3A504E-606E-4870-AF91-F87A48708C69}, id 0
<ul style="list-style-type: none"> <li> <ul style="list-style-type: none"> <li>Ethernet II, Src: IntelCor_ce:30:8d (f8:16:54:ce:30:8d), Dst: Nomadix_03:6b:11 (00:50:e8:03:6b:11) <ul style="list-style-type: none"> <li>Destination: Nomadix_03:6b:11 (00:50:e8:03:6b:11)</li> <li>Source: IntelCor_ce:30:8d (f8:16:54:ce:30:8d)</li> <li>Type: IPv4 (0x0800)</li> </ul> </li> <li>Internet Protocol Version 4, Src: 172.20.3.232, Dst: 64.13.139.230</li> <li>Transmission Control Protocol, Src Port: 52554, Dst Port: 23, Seq: 253, Ack: 16836, Len: 1</li> <li> <ul style="list-style-type: none"> <li>Telnet <ul style="list-style-type: none"> <li>Data: p</li> </ul> </li> </ul> </li> </ul> </li> </ul>
[Community ID: 1:CnE5b/nT6cD2hmPK/PKzWb5jLU=]

```

> Frame 23516: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{7F3A504E-606E-4870-AF91-F87A48708C69}, id 0
✓ Ethernet II, Src: IntelCor_ce:30:8d (f8:16:54:ce:30:8d), Dst: Nomadix_03:6b:11 (00:50:e8:03:6b:11)
  > Destination: Nomadix_03:6b:11 (00:50:e8:03:6b:11)
  > Source: IntelCor_ce:30:8d (f8:16:54:ce:30:8d)
  Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 172.20.3.232, Dst: 64.13.139.230
> Transmission Control Protocol, Src Port: 52554, Dst Port: 23, Seq: 254, Ack: 16837, Len: 1
✓ Telnet
  Data: s
[Community ID: 1:CnE5b/nT6cD2hmPK/PKzWwB5jLU=]

> Frame 23518: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{7F3A504E-606E-4870-AF91-F87A48708C69}, id 0
✓ Ethernet II, Src: IntelCor_ce:30:8d (f8:16:54:ce:30:8d), Dst: Nomadix_03:6b:11 (00:50:e8:03:6b:11)
  > Destination: Nomadix_03:6b:11 (00:50:e8:03:6b:11)
  > Source: IntelCor_ce:30:8d (f8:16:54:ce:30:8d)
  Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 172.20.3.232, Dst: 64.13.139.230
> Transmission Control Protocol, Src Port: 52554, Dst Port: 23, Seq: 255, Ack: 16838, Len: 1
✓ Telnet
  Data: c
[Community ID: 1:CnE5b/nT6cD2hmPK/PKzWwB5jLU=]

> Frame 23544: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{7F3A504E-606E-4870-AF91-F87A48708C69}, id 0
✓ Ethernet II, Src: IntelCor_ce:30:8d (f8:16:54:ce:30:8d), Dst: Nomadix_03:6b:11 (00:50:e8:03:6b:11)
  > Destination: Nomadix_03:6b:11 (00:50:e8:03:6b:11)
  > Source: IntelCor_ce:30:8d (f8:16:54:ce:30:8d)
  Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 172.20.3.232, Dst: 64.13.139.230
> Transmission Control Protocol, Src Port: 52554, Dst Port: 23, Seq: 256, Ack: 16839, Len: 1
✓ Telnet
  Data: 6
[Community ID: 1:CnE5b/nT6cD2hmPK/PKzWwB5jLU=]

> Frame 23547: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{7F3A504E-606E-4870-AF91-F87A48708C69}, id 0
✓ Ethernet II, Src: IntelCor_ce:30:8d (f8:16:54:ce:30:8d), Dst: Nomadix_03:6b:11 (00:50:e8:03:6b:11)
  > Destination: Nomadix_03:6b:11 (00:50:e8:03:6b:11)
  > Source: IntelCor_ce:30:8d (f8:16:54:ce:30:8d)
  Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 172.20.3.232, Dst: 64.13.139.230
> Transmission Control Protocol, Src Port: 52554, Dst Port: 23, Seq: 257, Ack: 16840, Len: 1
✓ Telnet
  Data: 2
[Community ID: 1:CnE5b/nT6cD2hmPK/PKzWwB5jLU=]

> Frame 23552: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{7F3A504E-606E-4870-AF91-F87A48708C69}, id 0
✓ Ethernet II, Src: IntelCor_ce:30:8d (f8:16:54:ce:30:8d), Dst: Nomadix_03:6b:11 (00:50:e8:03:6b:11)
  > Destination: Nomadix_03:6b:11 (00:50:e8:03:6b:11)
  > Source: IntelCor_ce:30:8d (f8:16:54:ce:30:8d)
  Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 172.20.3.232, Dst: 64.13.139.230
> Transmission Control Protocol, Src Port: 52554, Dst Port: 23, Seq: 258, Ack: 16841, Len: 1
✓ Telnet
  Data: 0
[Community ID: 1:CnE5b/nT6cD2hmPK/PKzWwB5jLU=]

> Frame 23556: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{7F3A504E-606E-4870-AF91-F87A48708C69}, id 0
✓ Ethernet II, Src: IntelCor_ce:30:8d (f8:16:54:ce:30:8d), Dst: Nomadix_03:6b:11 (00:50:e8:03:6b:11)
  > Destination: Nomadix_03:6b:11 (00:50:e8:03:6b:11)
  > Source: IntelCor_ce:30:8d (f8:16:54:ce:30:8d)
  Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 172.20.3.232, Dst: 64.13.139.230
> Transmission Control Protocol, Src Port: 52554, Dst Port: 23, Seq: 259, Ack: 16842, Len: 1
✓ Telnet
  Data: 0
[Community ID: 1:CnE5b/nT6cD2hmPK/PKzWwB5jLU=]

```

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.

```

> Frame 28531: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{7F3A504E-606E-4870-AF91-F87A48708C69}, id 0
▼ Ethernet II, Src: Nomadix_03:6b:11 (00:50:e8:03:6b:11), Dst: IntelCor_ce:30:8d (f8:16:54:ce:30:8d)
  > Destination: IntelCor_ce:30:8d (f8:16:54:ce:30:8d)
  > Source: Nomadix_03:6b:11 (00:50:e8:03:6b:11)
  Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 64.13.139.230, Dst: 172.20.3.232
> Transmission Control Protocol, Src Port: 23, Dst Port: 52554, Seq: 17687, Ack: 390, Len: 1460
▼ Telnet
  Data: 2048 sliding tile puzzle game \r\n
  Data: ? show command list \r\n
  Data: aquarium an aquarium/sea animation in ASCII art \r\n
  Data: aquarium /mono monochrome mode, no colors \r\n

> Frame 28533: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{7F3A504E-606E-4870-AF91-F87A48708C69}, id 0
▼ Ethernet II, Src: Nomadix_03:6b:11 (00:50:e8:03:6b:11), Dst: IntelCor_ce:30:8d (f8:16:54:ce:30:8d)
  > Destination: IntelCor_ce:30:8d (f8:16:54:ce:30:8d)
  > Source: Nomadix_03:6b:11 (00:50:e8:03:6b:11)
  Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 64.13.139.230, Dst: 172.20.3.232
> Transmission Control Protocol, Src Port: 23, Dst Port: 52554, Seq: 19147, Ack: 390, Len: 1460
▼ Telnet
  Data: print day and time \r\n
  Data: ddate convert Gregorian dates to Discordian dates \r\n
  Data: delta convert to delta time \r\n
  Data: df show disk usage \r\n

> Frame 28534: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{7F3A504E-606E-4870-AF91-F87A48708C69}, id 0
▼ Ethernet II, Src: Nomadix_03:6b:11 (00:50:e8:03:6b:11), Dst: IntelCor_ce:30:8d (f8:16:54:ce:30:8d)
  > Destination: IntelCor_ce:30:8d (f8:16:54:ce:30:8d)
  > Source: Nomadix_03:6b:11 (00:50:e8:03:6b:11)
  Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 64.13.139.230, Dst: 172.20.3.232
> Transmission Control Protocol, Src Port: 23, Dst Port: 52554, Seq: 20607, Ack: 390, Len: 1460
▼ Telnet
  Data: c[uc|title] <text> display or transform a line of text \r\n
  Data: eliza converse with an AI psychotherapist \r\n
  Data: exit terminate and return to previous shell or logout \r\n
  Data: factor <number> print the prime factors of a number \r\n

```

- 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	<p>*Passwords cannot be used if they are susceptible to dictionary attacks.</p> <p>Account Creation Requires E-Mail Verification.</p>



## Create your CNN account

Already have an account? [Log in.](#)



Password is required

By clicking 'Create account', you agree to the [Terms of Use](#) and acknowledge the [Privacy Policy](#).

Create account

This site is protected by reCAPTCHA, and the Google [Privacy Policy](#) and [Terms of Service](#) apply.

- ✗ Use at least 12 characters
- ✗ Use upper or lower case characters
- ✗ Use one or more numbers
- ✗ Use special characters



## Reset your password

Can't remember your password? Enter your email address and we will send you an email to create a new password.




Send reset link

## Join Now — It's Free & Easy!

Username	<input type="text" value="SethiClemson1"/>	✓
Email	<input type="text" value="sethi@clemson.edu"/>	✓
Password	<input type="password" value="aaaaaa"/>	🔒
Skill Level	<input type="text" value="New to Chess"/>	▼


Create Your FREE Account

Or sign up using...

 Facebook  Google  Apple ID

I accept the site [Terms of Service](#) and agree to the [Privacy Policy](#).

## Forgot Password?

<input type="text" value="SethiClemson"/>
<input type="text" value="sethi@clemson.edu"/>

<input type="text" value="8e4pe"/>

Submit

Welcome to GitHub!  
Let's begin the adventure

Enter your email  
✓ sethi@clemson.edu

Create a password  
→ ●●●●●●●●●●●●●●●●

Continue

Password may be compromised  
Password is in a list of passwords commonly used on other websites



Welcome to GitHub!  
Let's begin the adventure

Enter your email  
✓ sethi@clemson.edu

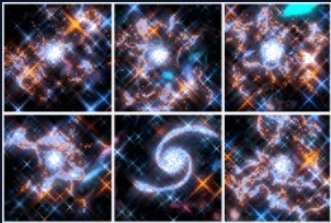
Create a password  
✓ ●●●●●●●●●●

Enter a username  
✓ SethiClemson

Would you like to receive product updates and announcements  
via email?  
Type "y" for yes or "n" for no  
✓ n

Verify your account

Pick the spiral galaxy



⌂ 🔊

# Whoa there!

You have exceeded a secondary rate limit.

Please wait a few minutes before you try again;  
in some cases this may take up to an hour.

[Contact Support](#) — [GitHub Status](#) — [@githubstatus](#)



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.

3. 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.

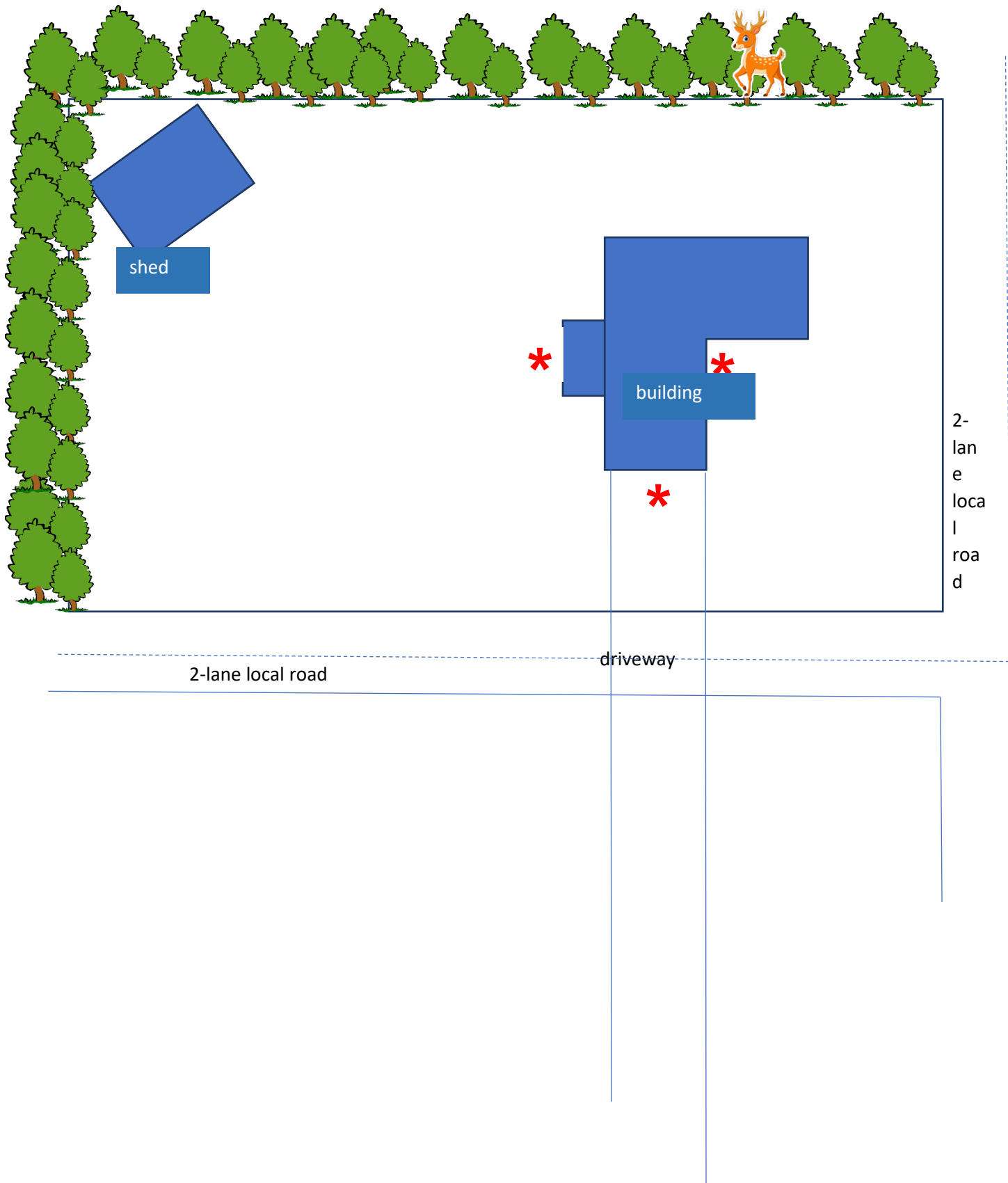
With civil unrest coming to large cities, the owners have a concern about their business being vandalized, burglarized, or destroyed. The two owners have hired you to design a comprehensive security system that includes both the exterior and the interior physical security. You were also asked to secure 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



## 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.



- 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
  - GFW 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>



- 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



Color: White



Bundle: Camera

- #4 in Surveillance Cameras
- Ring · Floodlight Cam · With Wi-Fi · With Audio · Outdoor Use · Motion Sensing · 270° field of view · Night Vision · Residential · Wireless

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

Blink Wireless Outdoor 2-Camera System

★★★★★ (4,774)



Motion Sensing · With Wi-Fi · Wireless · Amazon Alexa · Residential

No more researching for outlets and no professional installation required - everything you need to get started is in the box. Battery life: with long-lasting battery life, outdoor runs for up to 2 years on a single set of AA lithium batteries (included).

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

SimpliSafe Home 10-pc. Security System with 1080p HD Security Camera

★★★★★ (197)



- 10-pc. security system with 1080p security camera
- One free month of 24/7 professional monitoring included (\$24.99 value)
- No long-term contracts or cancellation fees
- Set it up in minutes with no tools or drilling required
- HD security camera with night vision and stainless steel privacy shutter

[More](#)

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.

The three suggested firewalls for Linux system are:



1.IPFire: IPFire is an open-source security tool for Linux developers. In addition to being a strong firewall, it serves as a VPN gateway, proxy server, and other network protection methods. IPFire must be installed on hardware or in virtual shells. IPFire is available for free download for running on-premise, as well as an AWS-based Linux firewall service.

2.Shorewall: Shorewall Firewall is an open-source security application that runs on top of Netfilter, the built-in firewall service included with Linux kernels 2.4 and later. Shorewall just requires an interface to customize your current security capabilities, thus it doesn't require any hardware or a virtualized shell. It comprises six packages, including basic functionality, firewall packages for IPv4 and IPv6, "light" and "full-feature" administration, and an event-reacting package.

3.Untangle NG Firewall complete: This Linux firewall system comprises more than 20 separate security programs, both free and commercial. You can install any of the free and premium components as stand-alone solutions, or you can pay a fixed amount for the entire package. Untangle also provides pre-bundled solutions for government and non-profit organizations who qualify.