CyberPatriot: Unplugged

Hey friends! It's your friendly neighborhood cyber nerd, here to prep you for an awesome opportunity: becoming a CyberPatriot! This booklet contains information adapted from the CyberPatriot training modules (plus a few other helpful hints) - it's meant to make training for CyberPatriot defensive competitions available for people without internet access at home.

Why Cybersecurity?

Have you ever thought about what can be affected by a cyber breach? It's not just having your password exposed - many attributes can be affected by a cyber attack! Your school, your parents' bank, your doctor's office, your local police and fire departments - all are at risk of cyber attacks if they use the internet. And, guess what? All of those places use the internet! In order to keep all of these establishments safe, each must have an understanding of cybersecurity. When you grow up, businesses will continue to need cybersecurity - perhaps even more than businesses need it today! This booklet will get you started on the road to cyber safety, whether just for your personal internet use or for your careers as adults.

The C.I.A. Triad

C - Confidentiality. In order to keep something confidential, you want to make sure you have *hidden* both your *data* and *resources.*

I - Integrity. This section has two parts: data integrity and origin integrity! In order to keep something's integrity your *data,* the data's *origin,* and general *resources* on your system must not have been *tampered with.*

A - Availability. In order to keep something available, you want to make sure your *data* and *resources* are always able to be *used.*

These principles describe how the ideal computer system would be set up - with only *approved* users able to *access* (C) and *change* (I) certain data and resources. And what use is data or a resource if it's unavailable? The answer: *useless* (A). When you put all three of these concepts together, you get the undeniable magic of the three pillars of cybersecurity.

A Few Computer Basics

You might be thinking, how does a computer even work? Well, don't worry; we'll break it down for you here with some definitions. Try and remember important terms so you can answer the questions without flipping back to the definitions!

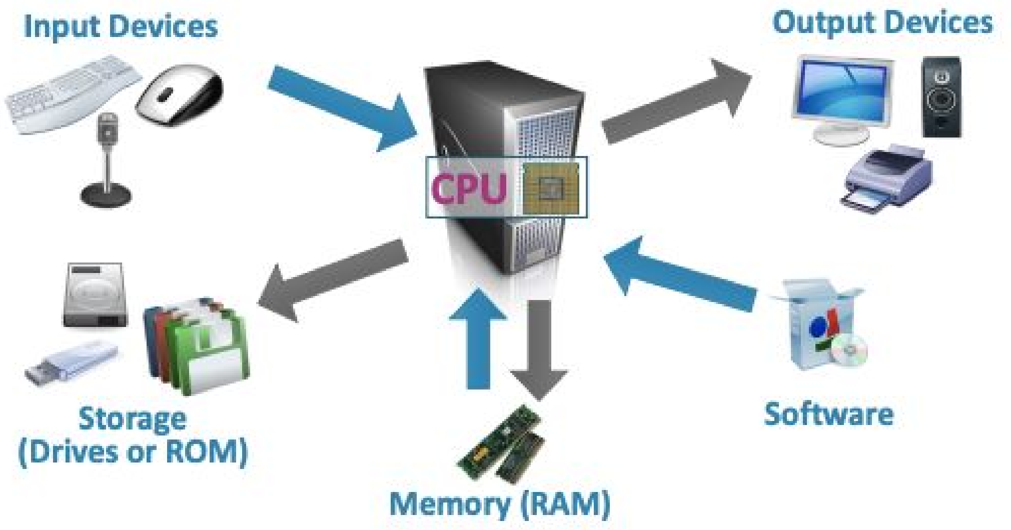
Central Processing Unit (CPU): This is kind of like your computer's brain! The power of the CPU will decide how fast the computer can process instructions. When the user states an instruction (through the keyboard or mouse), the CPU tells other parts of your computer how to work through the instruction you gave it.

Read-Only Memory (ROM): As the name states, this memory is read-only. Since all you can do is read it, its data does not change very frequently. ROM's main purpose is to store firmware - software that is closely tied to hardware, and unlikely to need frequent updates.

Random Access Memory (RAM): Just like you have a short-term and long-term memory, your computer does too. RAM is the computer's short-term memory! It will save your state in various software programs, so you can access that saved state whenever you'd like to come back to it. However, this memory isn't long-term - RAM is refreshed when you turn your computer off.

Operating System (OS): Kind of like the "template" of your computer. It makes all the computer's resources work together so you can use your system easily! The OS allows users to personalize settings without permanently changing them, and its easy-to-understand template allows users without technological experience (like your grandma!) to use the computer with no trouble.

Basic Input-Output System (BIOS): The BIOS lets your OS connect to devices that process input, output, and storage - it is a permanent part of your computer! It will manage some basic computer settings that every system needs, like the date, time, and management of power usage. The BIOS is a piece of software.



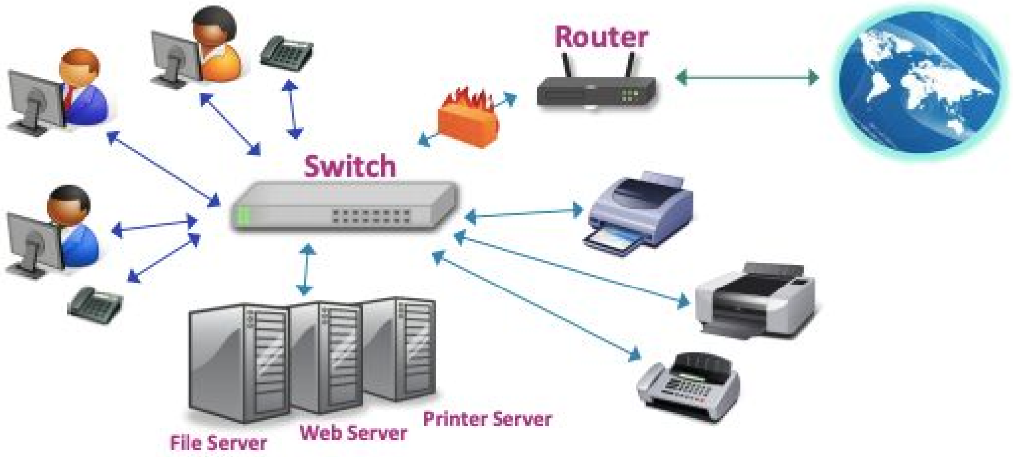
Thank you to the CyberPatriot website for this helpful graphic!
[Here, we switch the topic to network basics!]

<u>Servers:</u> These are computers that decide to manage resources that are shared between them. A network may have a file server, web server, and printer server - all separate from each other, but working towards the same goal.

<u>Switch:</u> There are two types of switches: managed, and unmanaged. A managed switch can be configured to help monitor the traffic within a network; an unmanaged switch requires no extra configuration and works immediately! For a personal, home network, you are more likely to use an unmanaged switch.

<u>Firewall:</u> You might have heard this term before - now to learn its definition. A firewall checks all the traffic headed toward the switch, to ensure that no incoming or outgoing traffic contains threatening material or odd characteristics. This keeps your network safe!

<u>Router:</u> While a switch controls traffic *within* a network, a router controls traffic *between* networks. Not only do they connect certain networks to each other, but they also connect the devices on those networks to the internet! Basically, all the inter-connection allows devices and networks to share just one internet connection - and this saves companies some big money when they use many devices.



Thank you to the CyberPatriot website for this helpful graphic as well!

[Here, we switch the topic to Virtual Machine basics!]

<u>Virtual Machine (VM):</u> If you complete this training module and decide that CyberPatriots is for you, you will use a VM in your competitions. A VM is an *environment* - an OS or a program - that does not exist physically, but rather is developed inside of another environment! A VM has zero resources that would make it self-sustaining: it relies on a physical computer (with its own separate OS) to run in completion. A VM is **also known as** an *image.*

Host: The operating system (OS) on the actual physical device where the virtual machine is installed.

Guest: The operating system (OS) that the virtual machine runs. The operating system of the host and guest do not have to be the same, but they are allowed to be the same if you so choose!

VMWare: A program that is used to both create and run virtual machines - VMWare is used to run VMs for CyberPatriot competitions. If you do compete, you'll be a champ with VMWare!

Alright, I think that's enough definitions to throw at you for now. Stand up, stretch for a minute, and then let's see if you remember any of this information! No flipping back, you promised!

But first, here's a thought-provoking question:
Do you know anyone (and I mean anyone!) who truly never uses a computer, or the internet, for absolutely anything? If you can prove it, write their name here:

[And don't forget - if a person isn't online at all, it means they have a greater chance of becoming a victim of identity theft! It's better to have a small online presence so you can be aware when an attacker tries to impersonate you. The last thing your grandpa needs is someone taking out a credit card in his name!]

Time to Test Your Skills!

Let's see if you've actually been paying attention so far! And after this, I promise we'll move on from the basics and into some more competition-specific content. You'll be ready to CyberPatriot it up in no time!

1) **Word Bank**

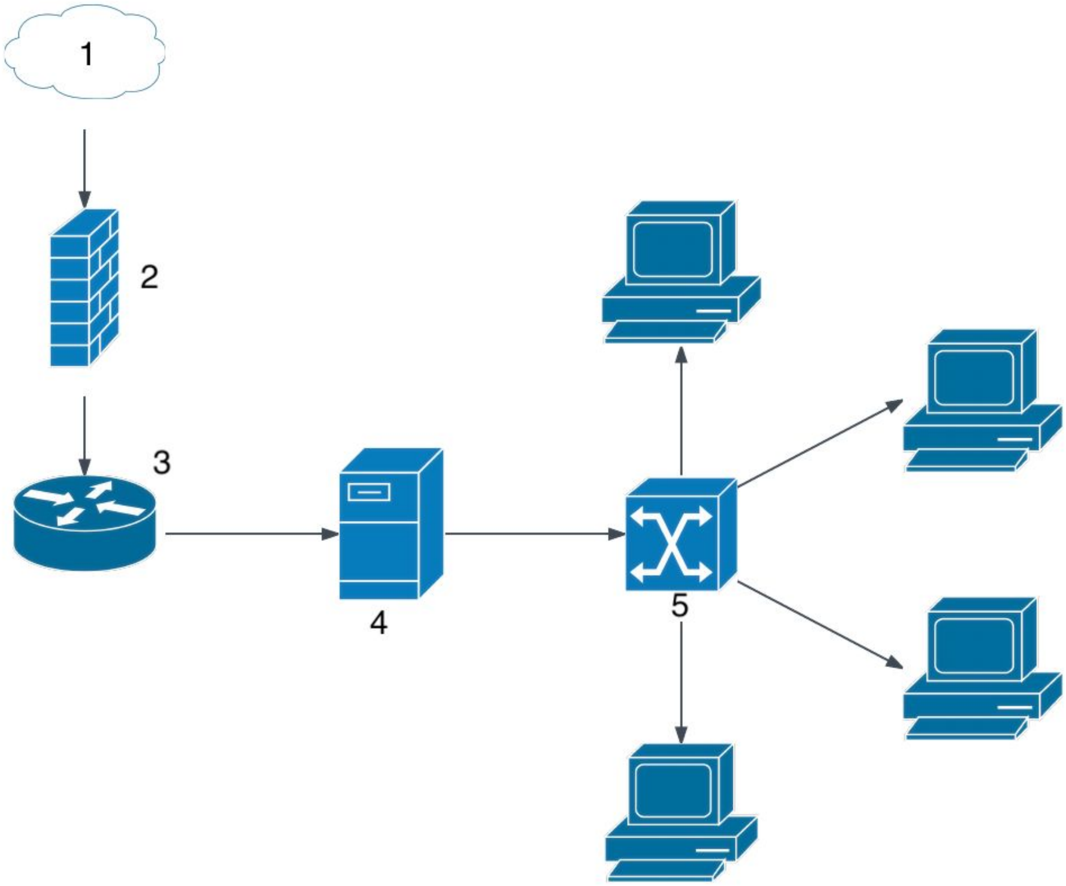
Switch RAM Guest OS BIOS Server
CPU Router Firewall Host ROM

Words Related to Networks	Words Related to Computer Systems

2) **Draw lines to match words with definitions. There might be a trick!**

Host	Environment that does not physically exist
Guest	Used to create and run something
Image	OS on the non-physical environment
VM	OS on the physical device
VMWare	Used to register contact info

3) Fill in the Blank



3.1)

3.2)

3.3)

3.4)

3.5)

Learning the Windows Operating System

Well, first things first, let's talk about customizing permissions in Windows! File permissions are an important part of protecting *data integrity* and *confidentiality* on your Windows machine. (I hope you remember those topics from earlier!) File permissions can **stop specific users, or a group of users,** from accessing or changing certain data on shared resources (like documents, spreadsheets, or applications). There are six types of file permissions, listed in order of commonality:

Read - allows a user to view, but not edit, attributes of a file or folder.
Write - allows users to change or even overwrite a file.
Execute - allows users to not only open a file, but to run it.
Modify - permission to change (but not delete) file's content, but cannot change its ownership.
List Folder Contents - names of files stored in a selected folder will be viewable by users given this permission.
Full Control - users have access to all controls (this is Administrator access).

In order to set permissions: right click on a folder, select "Properties", then click the Security tab.

Here's an exercise to test your knowledge (and remember these permissions, they're not just for Windows!):

4) Alice, Bob, and Eve require different permissions on the computer. Set permissions (by filling in the correct box) so that Eve has all permissions, Bob can read and write, and Alice can only read.

	Read	**Write**	**Execute**
Alice			
Bob			
Eve			

Now, another important topic: performance monitoring! Monitoring your CPU's performance allows you to track how both hardware and software are being used, and how they are performing. You can track the history of performance, but also see real-time activity! It's useful to see both of these, because it allows you to predict problems that may occur in the future - or to conduct forensics to stop potential attacks, and shut down vulnerabilities. Monitoring the performance can also help you decide if your hardware or software need to be updated!

You want to know a tool incredibly useful for monitoring performance? The task manager! It helps you do everything we just described! Along with showing current processes and programs running on the computer, it also shows network activity and how your resources are being used. There are two ways to open the task manager:

Right click on the Menu Bar, and then click Task Manager.

Or, hit **Ctrl+Alt+Delete** and select "Start Task Manager."

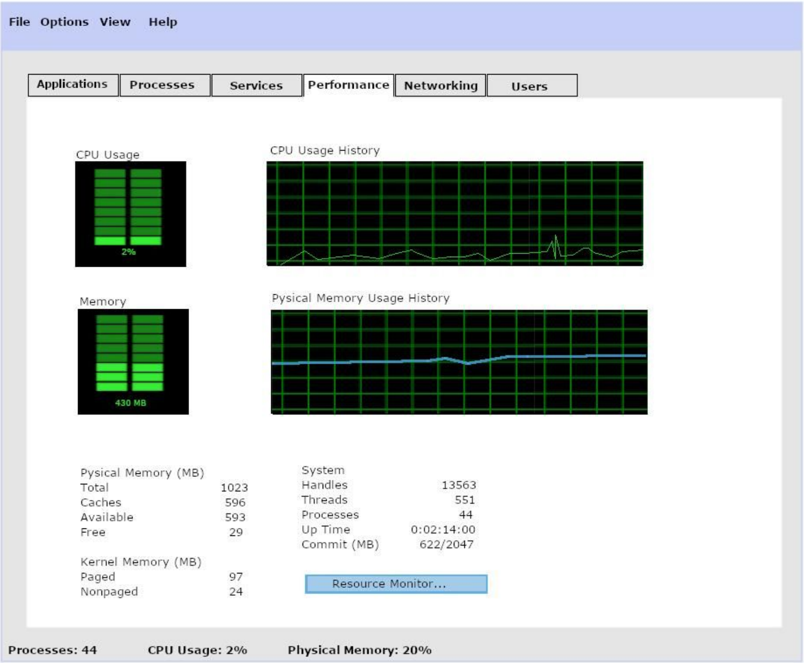
The task manager is capable of many different tasks, such as: closing programs that are not responding, checking to see if any software is running that is unnecessary, and to find processes that are associated with certain software (so you don't accidentally shut down the wrong application!). While there are many different tabs in the task manager that can be useful, we're only going to go over the Performance and Networking tabs in this booklet.

Another important use the task manager has is checking for malware. It can help show the usage of your CPU, and how much of your total available memory is being used. This can help you identify possible malware that could be running in your system! By checking under the "*Performance*" tab, you can see how much memory your entire OS is using. If the numbers are oddly high, there could be malware on your computer that's preventing it from running effectively! And as we all (hopefully) know, that's certainly not good.

Next to the "*Performance*" tab, you will find the "*Networking*" tab. The chart shows your current network connectivity. You may find signs of malware from here if you are seeing high peaks in the data, but you aren't currently using any programs connected to the internet.

Now, did you get all that? I'm gonna ask you a few questions just to make sure you understand what we discussed!

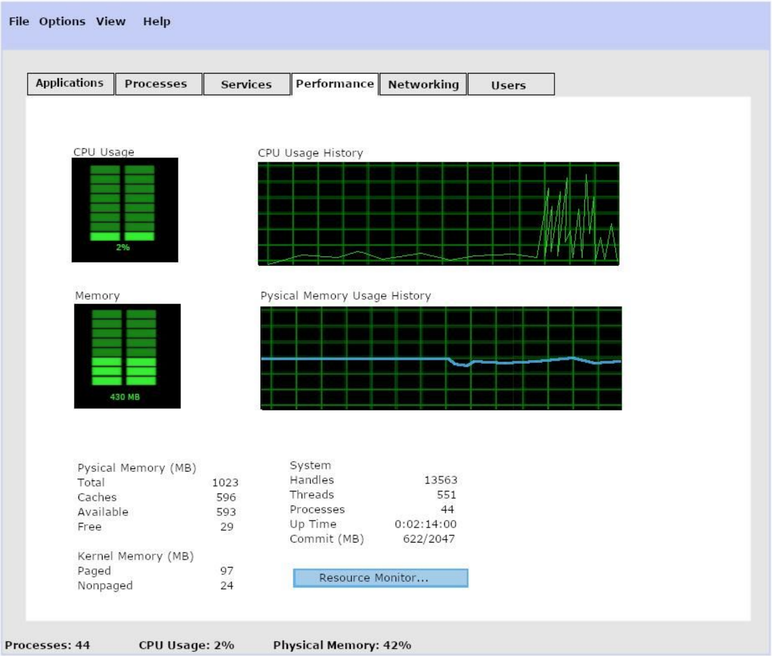
5) Which of these CPUs would most likely be infected with malware based off of the information in their "*Performance*" tab?



```
Pysical Memory (MB)              System
Total           1023             Handles            13563
Caches           596             Threads              551
Available        593             Processes             44
Free              29             Up Time      0:02:14:00
                                 Commit (MB)    622/2047
Kernel Memory (MB)
Paged             97
Nonpaged          24

Processes: 44     CPU Usage: 2%     Physical Memory: 20%
```

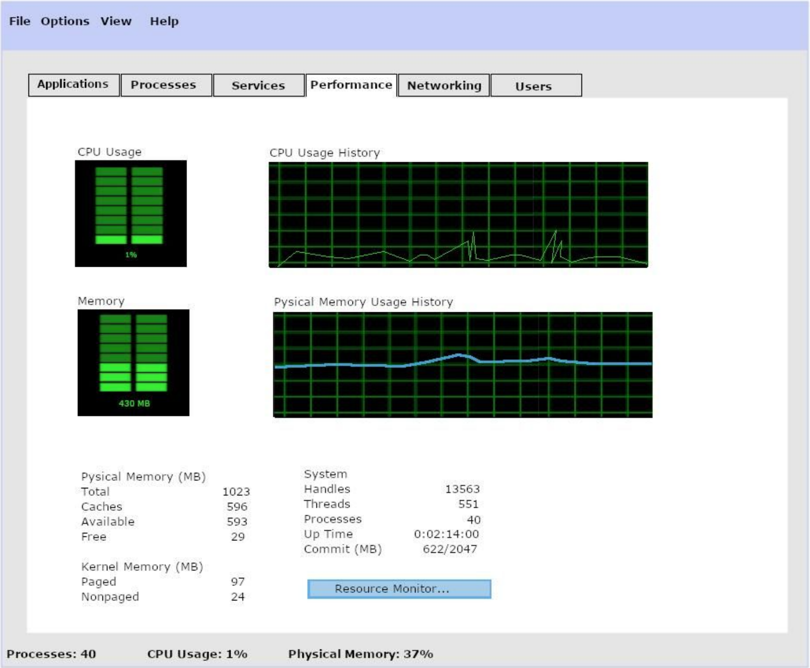
(A)



```
Pysical Memory (MB)              System
Total           1023             Handles            13563
Caches           596             Threads              551
Available        593             Processes             44
Free              29             Up Time      0:02:14:00
                                 Commit (MB)    622/2047
Kernel Memory (MB)
Paged             97
Nonpaged          24

Processes: 44     CPU Usage: 2%     Physical Memory: 42%
```

(B)

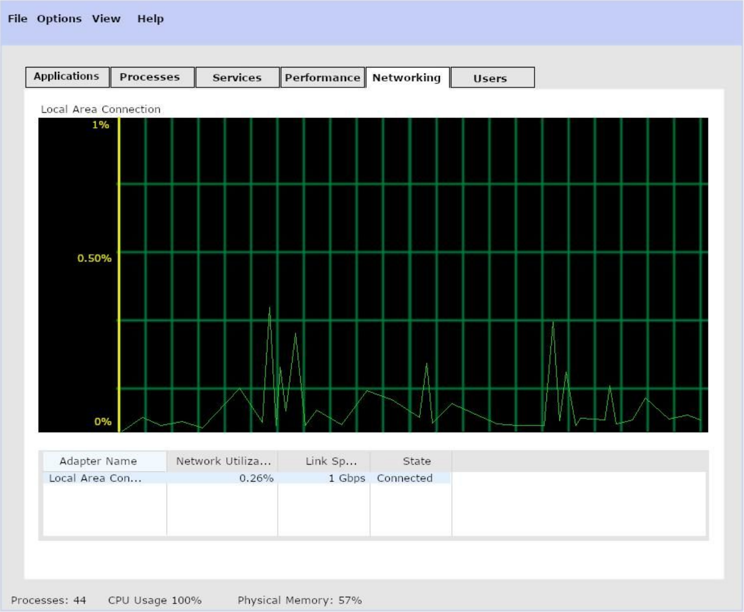


```
Pysical Memory (MB)              System
Total           1023             Handles            13563
Caches           596             Threads              551
Available        593             Processes             40
Free              29             Up Time      0:02:14:00
                                 Commit (MB)    622/2047
Kernel Memory (MB)
Paged             97
Nonpaged          24

Processes: 40     CPU Usage: 1%     Physical Memory: 37%
```

(C)

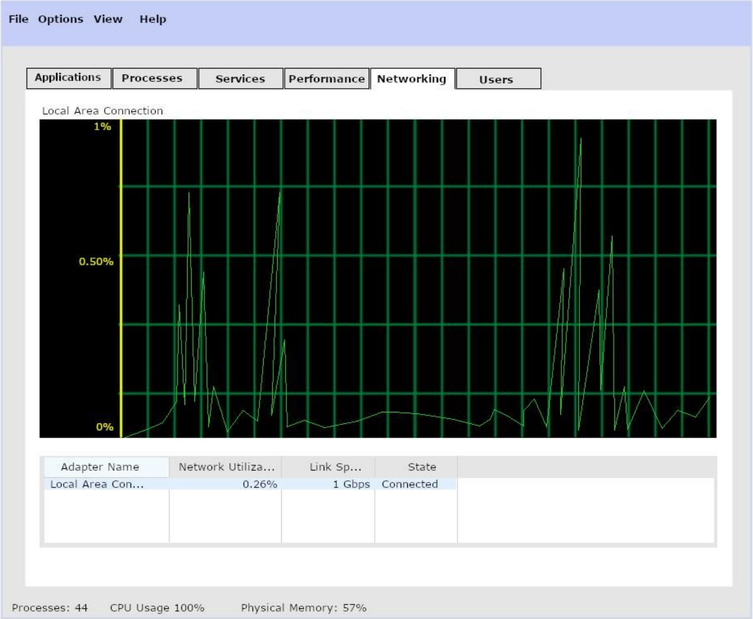
6) Which of these CPUs would most likely be infected with malware based off of the information in their "*Networking*" tab?



Adapter Name	Network Utiliza...	Link Sp...	State
Local Area Con...	0.26%	1 Gbps	Connected

Processes: 44 CPU Usage 100% Physical Memory: 57%

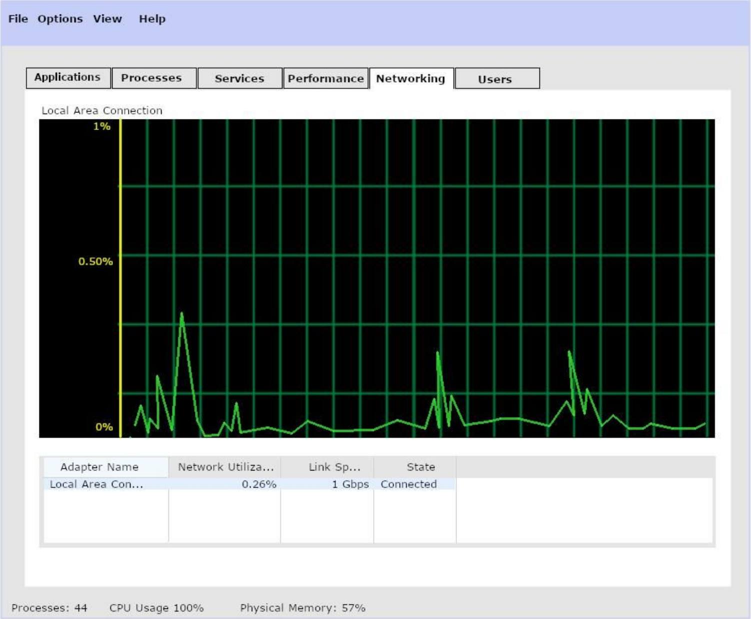
(A)



Adapter Name	Network Utiliza...	Link Sp...	State
Local Area Con...	0.26%	1 Gbps	Connected

Processes: 44 CPU Usage 100% Physical Memory: 57%

(B)



Adapter Name	Network Utiliza...	Link Sp...	State
Local Area Con...	0.26%	1 Gbps	Connected

Processes: 44 CPU Usage 100% Physical Memory: 57%

(C)

You've been doing great kids! We're almost done learning about Windows. Just one more pretty important topic: the command line. It can be an incredibly useful tool! While it's more commonly introduced in Linux systems (watch out for that topic later!), it can be super useful on Windows as well. In this section, we'll cover some different basic commands that can be useful to you in protecting your information, and tracking down malware that may be running on your computer. The commands we will cover are as follows: cipher, fc, and netstat.

Cipher

When you delete files off of your mechanical hard drive, they're actually **not** deleted immediately! While the space on your computer is freed up for your use, the files remain until the system overwrites them with new data. To clear these files immediately, Windows gives you a handy dandy feature we call cipher. To use it, open up your terminal. Then, you simply type:

```
cipher /w:C____
```

Cipher starts the program, while '/w' will removed unused data on the disk space. 'C' tells the terminal which drive to carry out this action on.

File Compare 'fc'

Another useful command to know is 'fc', which you can use to identify differences between two text files. It's particularly helpful for programmers if they are trying to find a difference between two versions of the same file. This would be a good way to identify if one version of a file has been tampered with!

There are two different ways to compare files: binary comparison and ASCII comparison. If one file has been changed, the prompt will display both texts; but if the files are matching, the prompt will simply state it as so.

For binary, follow your fc command with

```
fc /b "example1.txt" "example2.txt"
```

And for ASCII, type this way:

```
fc /l "example1.txt" "example2.txt"
```

"netstat"

Netstat is a great command to use if you want to quickly try to identify any open connections on your computer that might be malicious. The command is as follows:

```
netstat -nao
```

Those extra commands, known as *parameters,* give us some more information. 'n' is what displays the active TCP connections. 'a' displays active TCP connection, with TCP/UDP ports the computer is listening to. Finally, 'o' includes the process ID for each connection, which helps you find the process in your task manager! If you'd like to learn about the other parameters that exist, make your way to this website: https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/netstat

[Helpful Hint: TCP stands for Transmission Control Protocol. It sends messages between applications. UDP stands for User Datagram Protocol. It gives port numbers for different user requests. A port identifies one computer in a connection between two computers.]

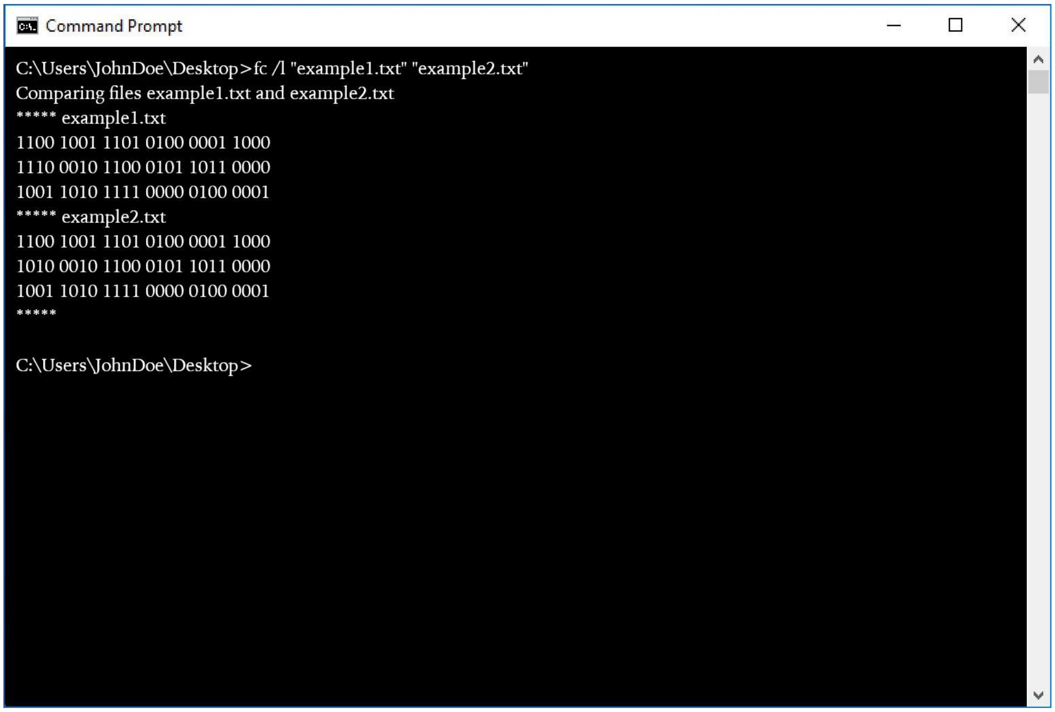
The first column in the output will be the protocol being used (TCP/UDP). The second is the local address and port number. The third is the foreign address and port number. Lastly, the fourth column is the state. Any unrecognized foreign addresses that are in an "established" state - or local connection with a strange port that says "Listening" *could* be a sign of an attacker compromising your system. This command is most useful if you know your system well, and know what connections generally occur.

Here's my last round of questions for Windows, to make sure you've been paying attention this whole time!

7) Write the command needed to clear deleted files from the D:/ drive.

8) Write the command needed to compare the binary output of two files: 'important_data_1' and 'important_data_2'

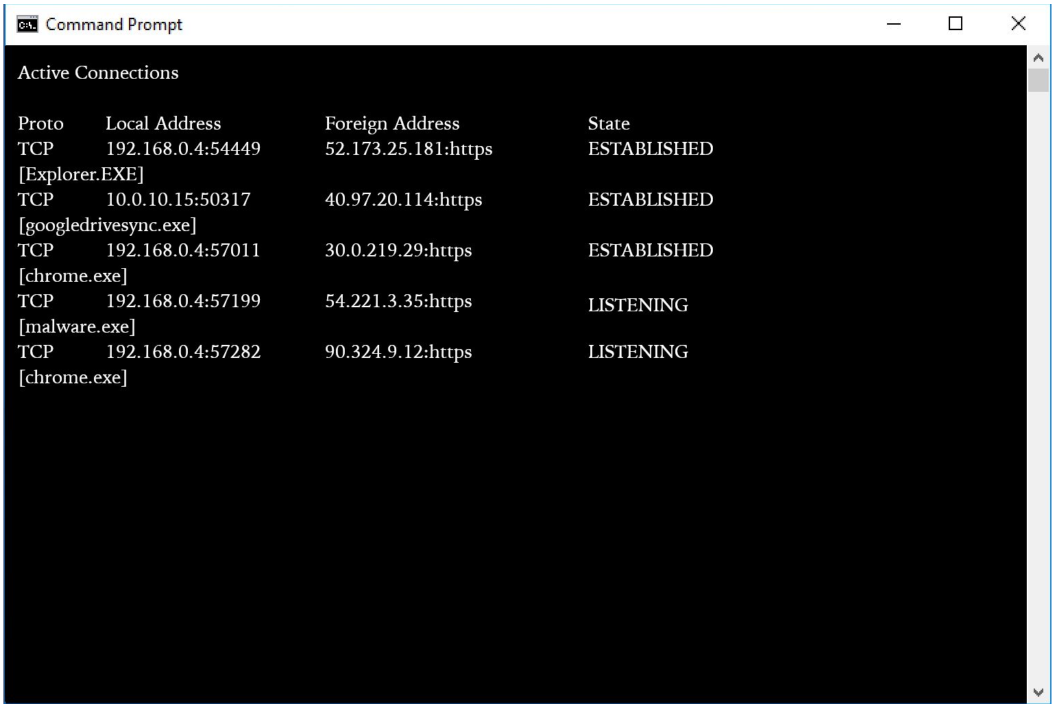
9) Without looking at the two files line by line, how can you tell one has been changed?



```
C:\Users\JohnDoe\Desktop>fc /l "example1.txt" "example2.txt"
Comparing files example1.txt and example2.txt
***** example1.txt
1100 1001 1101 0100 0001 1000
1110 0010 1100 0101 1011 0000
1001 1010 1111 0000 0100 0001
***** example2.txt
1100 1001 1101 0100 0001 1000
1010 0010 1100 0101 1011 0000
1001 1010 1111 0000 0100 0001
*****

C:\Users\JohnDoe\Desktop>
```

10) After typing in the 'netstat' command, the following information is outputted. Can you identify any possible malicious connections? If so, what tipped you off to them being malicious?



```
Active Connections

Proto    Local Address          Foreign Address         State
TCP      192.168.0.4:54449      52.173.25.181:https     ESTABLISHED
[Explorer.EXE]
TCP      10.0.10.15:50317       40.97.20.114:https      ESTABLISHED
[googledrivesync.exe]
TCP      192.168.0.4:57011      30.0.219.29:https       ESTABLISHED
[chrome.exe]
TCP      192.168.0.4:57199      54.221.3.35:https       LISTENING
[malware.exe]
TCP      192.168.0.4:57282      90.324.9.12:https       LISTENING
[chrome.exe]
```

Learning the Ubuntu Operating System

You've almost learned everything you need to know to start off your first CyberPatriot meeting with a leg up! After mastering the basics (which I'm sure you have) and learning a bit about Windows, you'll now get to dive deep into the specific flavor of Linux used for CyberPatriot: Ubuntu.

Linux encompasses a family of OSs modeled off of the Unix OS. Linux performs many of the same functions as OS X or Windows. However, Linux is special! It's open-source. AKA, you can download it for free! Anyone can use the Linux kernel, modify it, or distribute it. Similarly, many different flavors of Linux and add-on programs for them are absolutely free! What is a kernel, you may ask? It's the main part of an operating system. The kernel manages resources like memory, input and output devices, and processes. It translates commands to be understood by your CPU!

Root is the Administrator account in Linux. There can actually be multiple roots in just one system! If you are a user with the root password, you can decide if you'd like actions to be carried out just as a user, or as the root instead. Using this technique will require a command you'll learn later.

Ubuntu: the most user-friendly flavor of Linux. The one we will be studying for the remainder of this booklet!

After that quick rundown, let's get into some topics similar to what you read earlier in the Windows section! Ubuntu makes good use of the command line. While using the command line requires a bit of effort - a reference to commands to use or straight up memorizing those commands - command line actually provides the user with more control over their system. In fact, for some operations in Ubuntu, command line is the *only way* to run them! If you want to use command line, but you want to streamline the process, you can do something called scripting. According to the CyberPatriot website, "scripts are sequenced lists of commands that allow users to send multiple commands at once." They can be used to monitor your computer, backup files, gather information, and so much more!

Another helpful hint: if you want to write commands in your terminal, those commands are **case sensitive**. Be sure to know which letters you need to use, the uppercase or lowercase! Otherwise, the commands you enter will behave unexpectedly or just not run. The *enter* key will start your command and *Ctrl+D* will close the running commands, or exit your terminal.
"sudo"

One pretty important command you can use in your terminal is the sudo command. It allows a user with root permissions (who is not actually the root user) to "level up" and run administrative commands with their own password, rather than the actual root user's password.

There's a spinoff of the sudo command as well! Its name isn't too hard to remember - the su option. It helps you cover all your bases - once you type in "sudo su" to your command line (and push enter), you no longer have to precede commands with "sudo" to run with root powers. Isn't that just so convenient?

Here are some websites you can use to learn even more about the Ubuntu terminal, if I have you intrigued! http://ubuntu-manual.org/, http://manpages.ubuntu.com/, and https://help.ubuntu.com/community/UsingTheTerminal.

Now, for a short questions break! Have you been paying attention?

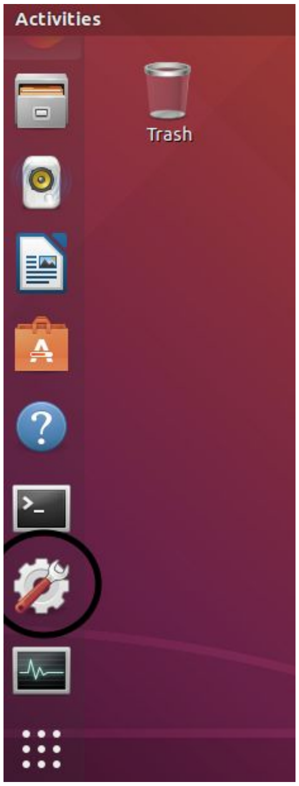
11) If the proper syntax for the command is "adduser," which of these (could be more than one) will run correctly if the user has root privileges, but is not the root user themselves?

A. sudo su
   adduser CyberNerd
B. AddUser CyberNerd
C. sudo su
   AddUser CyberNerd
D. adduser CyberNerd
E. sudo adduser CyberNerd
F. sudo AddUser CyberNerd

12) Which operating systems can make use of the command line?

A. Windows OS
B. Linux OSs (of any flavor)
C. Mac OS
D. All of the above
E. None of the above
   (one of these we haven't talked about, but use your best guess! I believe in you!)

Very good! Let's continue on with learning more about Ubuntu security. Now, a good tidbit to know - Linux OSs do not have a control panel like the Windows system does. So how are we supposed to change our system? Well, the answer lies here - in System Settings. (see circled, below. *Above that is the terminal icon!*)



Once you click on this icon, you should navigate to "User Settings" and restrict root privileges, as well as password protect all accounts in the system. This will keep your system secure and safe!

But now that that's taken care of, let's go back to a couple of **super important** command line tasks.

Turning On the Firewall

To prevent unallowed access to your system, activate the Ubuntu Built-in Firewall (UFW). In order to do this, you'll have to download Gufw! Open your terminal and type "sudo apt-get install gufw" in the command line. You'll be prompted to input your password to download the gufw. Gufw is a graphical firewall interface that you can retrieve from the Software Center. Once the Gufw is fully loaded, click those nine dots in the corner (of the left image) and search "Firewall Configuration". A new window will pop open, and you just turn "on" the firewall with its switch! Who knew protecting your computer could be so simple?

The "gedit" Command

Gedit is one among multiple text editing commands in the Ubuntu system. To use it, you'll type `gedit [filepath]` What makes gedit stand out among other text editors is the fact that it will cause a second window to open - this means you can more easily update the text of a file! [Helpful Hint: before you ever try to use gedit, navigate to Edit → Preferences and uncheck "Create a backup copy of files" - this will help you avoid saving issues.] It may seem meek, but gedit is incredibly useful. Even though it's a text editor, there are important things stored in your computer in text files! To learn a few important things you can use gedit to do, read below and then flip onto the next page.

Pluggable Authentication Modules [PAM] are used for applications and logging on. PAM Files cannot grant or remove new privileges to users, but they help simplify authentication! If you want to create password restrictions (based on prior passwords used, password length, and password complexity), you'll need to edit the PAM Password file. Type this command:

```
gedit /etc/pam.d/common-password
```

(Quick note - if a line starts with a hashtag "#", those are just comments to help you understand the file. Ignore those!) If you want to keep track of the user's previous passwords up to four, you should add "remember=4" to the end of the line that has "pam_unix.so". If you want a minimum length of 10 for all user's passwords, add "minlen=10" to the end of that same line mentioned a second ago. Using these tricks will help ensure all users of your system are using strong and fresh passwords!

Just like Windows, the guest account in Ubuntu is turned on by default! In order to prevent people getting onto your computer and hiding their identity, you need to turn that thing off. To turn off the guest account, open your terminal and type this command:

```
gedit /etc/lightdm/lightdm.conf
```

(Once a second window pops up, add the line **allow-guest=false** to the file's end.) This command probably doesn't make sense to you, does it? Well, let me elaborate! The guest account is controlled by something called LightDM - it's the display manager that runs your computer's login screen. But, I bet the text you added to the file made sense - simply, we don't want to allow the guest account to run. Restart your system and the guest account should not be available!

Let's see what you've comprehended -

13) Which command gives a user root privileges? (Tell me you remember!)

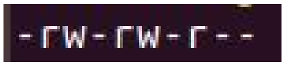
14) Can you automatically turn on your firewall, with no previous actions necessary? If you must take actions, what are they?

15) What is special about the gedit text editor?

"ls" command

An extremely useful command in Ubuntu (which is also the first command you would be taught in a Linux class) is the **ls** command. It must always be a lowercase l and s - remember how we talked about syntax? This command will list out the properties and contents of a directory or file! `ls [option] [filepath]`
One common option you will use is **-l.** This option will provide you with even more details than the ls command by itself. In order, you should receive these details: permissions, links to the file, user that made the file, the group the user was in when the file was created, the size of the file in kilobytes, the date the file was modified, and finally, the name of the file.

Another reference to information from earlier - remember talking about file permissions in Windows? Instead of using a table, here's another way to think about them. When you use the ls-l command on a file, the first thing that pops up is the file's permissions. They should look something like this:



```
-rw-rw-r--
```

The first character refers to if the object is a directory or a file. A dash represents a file, and a "d" represents a directory. The next three characters are the user permissions, the three after that are the group permissions, and the last three are the permissions of other users on that item. Not too hard to keep up with, I think!

"chmod" command

Short, but sweet: the chmod command allows you to change permissions for your files! You can change permissions for the user, group, or others, adding(+) or subtracting(-) them, and you must specify which privileges are being changed (read, write, execute). An example command would look like this:
`chmod o+w details.text` (This would add write privileges for other users.)

"netstat" command

Hopefully you'll recall this command from the Windows section! Like many other commands, it is quite useful in Linux systems as well. There are several options you can use with netstat that aid in securing your system.
In order to use this command, you may first have to install the package - use the command `apt install net-tools`
After your installation is complete, there are several useful commands to implement with netstat: netstat -at, netstat -au, netstat -tp, and netstat -s.
`netstat -at` will list all the Transmission Control Protocol (TCP) port connections.

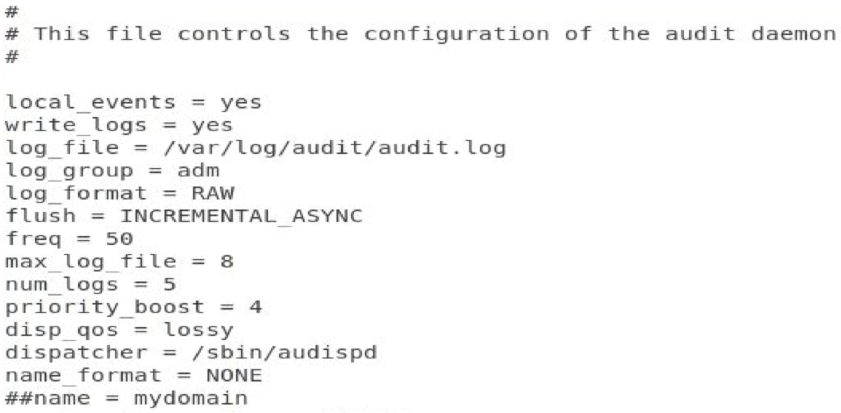
netstat -au will list all the User Datagram Protocol UDP) port connections.
netstat -tp will display all the running services with their Process IDs. And finally, netstat -s will show you all the relevant statistics of your system and its various protocols, in case you'd like to see multiple at once. All of these commands can be used to help identify if there are ports open or services running that should not be open or used at that time!

Four Types of System Logs

If you open up the Ubuntu menu (remember that? The nine dots?) and type "System Log" in the search field, you'll be able to view the available system logs! There are four types: **sys.log** (keeps track of operating system events), **dpkg.log** (keeps track of software events like installations), **Xorg.0.log** (keeps track of desktop events like graphic card errors), and **auth.log** (tracks events that prompt users for passwords, like using sudo!). If any part of your system gives you an error, whether expected or unexpected, it will be stored in these logs. This helps you identify whether or not things are acting as they should be! Similarly, if your desktop or an application shuts down, you can scan the logs to pinpoint exactly what went wrong.

Lastly... Audit Policies

In Windows, auditing is set up by default. Not in Ubuntu! But don't worry, there's a short process to setting up audits. First, you'll have to install the auditing program: apt-get install auditd [Similar to above, if this doesn't work, prefix the command with "sudo"] Next, in the terminal, enable audits with the command auditctl -e 1 Finally, in order to view and change the policies on your system, run this command:
gedit /etc/audit/auditd.conf The file that opens should look something like this, with extra lines at the end of the file.



```
#
# This file controls the configuration of the audit daemon
#

local_events = yes
write_logs = yes
log_file = /var/log/audit/audit.log
log_group = adm
log_format = RAW
flush = INCREMENTAL_ASYNC
freq = 50
max_log_file = 8
num_logs = 5
priority_boost = 4
disp_qos = lossy
dispatcher = /sbin/audispd
name_format = NONE
##name = mydomain
```

Last Time to Test Your Skills!

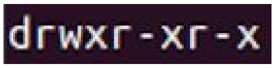
16) Which command will list out the properties and contents of a file or directory?

a. ls
b. netstat
c. ls -l
d. chmod

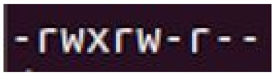
17) What types of system logs are automatically included when you download Ubuntu? (Circle all that apply.)

a. sys.log
b. meme.log
c. auth.log
d. dpkg.log
e. ubu.log

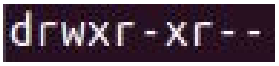
18) Which of the following options shows read, write, and execute permissions for the user, read and write permissions for the group, and read permissions for others (of a file?)

a. 

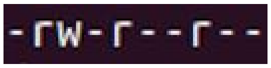
```
drwxr-xr-x
```

b. 

```
-rwxrw-r--
```

c. 

```
drwxr-xr--
```

d. 

```
-rw-r--r--
```

19) Which command would you use to change permissions of a file or directory?

a. sudo
b. chmod
c. ls
d. netstat

20) True or False:

a. Auditing is automatically set up in Ubuntu.
b. One type of system log is "Xorg.2.log".
c. "-l" is a common option to use with the "ls" command.
d. It is useful to know which services are running.

CONGRATS! If you made it this far, this cyber nerd is incredibly proud of you. I hope you're also proud of what you've learned. Flip to the next page for resources that you can use to keep on learning about cybersecurity.

List of References

Just in case I have you hooked and you'd like some resources to check out on your own, here are the references we used to create this booklet! Some are from the official CyberPatriot website, but others are a bit more random. They'll have all the information you need, and even more than necessary to compete with CyberPatriot teams. Let's get nerdy! Thanks again, and farewell!

- **Introduction to Computer Security by Matt Bishop (Chapter 1)**
- https://www.uscyberpatriot.org/home
- https://s3.amazonaws.com/cpvii/Training+materials/Unit+One+-+Introduction+to+CyberPatriot+and+Cyber+Security.pdf
- https://s3.amazonaws.com/cpvii/Training+materials/Unit+Four+-+Principles+of+Cybersecurity.pdf
- https://s3.amazonaws.com/cpvii/Training+materials/Unit+Five+-+Microsoft+Windows+Security.pdf
- https://s3.amazonaws.com/cpvii/Training+materials/Unit+Six+-+Windows+File+Protections+and+Monitoring.pdf
- https://s3.amazonaws.com/cpvii/Training+materials/Unit+Seven+-+Introduction+to+Linux+and+Ubuntu.pdf
- https://s3.amazonaws.com/cpvii/Training+materials/Unit+Eight+-+Ubuntu+Security.pdf
- https://210geeks.com/blogs/news/basic-computer-anatomy-101
- https://en.wikipedia.org/wiki/Read-only_memory
- https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/networking-basics.html
- https://www.tecmint.com/20-netstat-commands-for-linux-network-management/

Images in the booklet were created by the authors or grabbed from these sites:

- https://www.centro.co.uk/it-solutions/virtual-machines/
- https://www.lucidchart.com/pages/templates/network-diagram/network-diagram-example-template
- https://s3.amazonaws.com/cpvii/Training+materials/Unit+Three+-+Computer+Basics+and+Virtual+Machines.pdf