!

Cybersecurity Notebook 2020 - 2021

Unit 1

Name:

Table of Contents

**Unit 1**

[Unit 1.1.1](#qj4ntvhaqz5x) Cybersecurity and Code of Conduct

[Unit 1.1.2](#i3z4xef4891l) Password Protection and Authentication

[Unit 1.1.3](#p4tvj2e9swtw) Email and Social Media Security Risks

[Unit 1.1.4](#uhwgzjkxodr1) Save the Day

[Unit 1.2.1](#1qiyr3bhgtfb) Firewalls and Malware

[Unit 1.2.2](#d2kr018ynmsq) File Management

[Unit 1.2.3](#7n6kyouxpw7y) Process Management

[Unit 1.2.4](#seumze5qbnmh) Securing Your Browser

[Unit 1.2.5](#y9ikqohzut0x) It’s a Trap!

[Unit 1.3.1](#zfakf3h5g7bx) Dangerous Situation

**Unit 1.1.1**

**Goals:**

* Define Cybersecurity.
* Identify insecure data sharing practices.
* Describe the impact of your digital presence.
* Begin creation of a classroom code of conduct addressing professional, ethical, and legal standards.

**Unit 1 Case**



## The Hacked Computer

**You are in your high school cafeteria one morning, planning to meet your friends. You decide to go get something to drink and leave your laptop out on the table. You figure you’ll only be away for a minute to two—What’s the worst that could happen? You get your drink, come back to the table, and see that your friends arrived while you were away. After chatting with them for a bit, you close your laptop and head off to your classes for the day. The next time you open your laptop, you notice a suspicious file on your Desktop that you’ve never seen before. You start to think about all of the information available and at risk on your computer and you begin to worry about how that file might have gotten on your computer.**

**But how can you figure out what might have been touched? How can you fix anything that has been altered? And most importantly, how can you keep this from happening again?**

**The activities and projects in this unit will arm you with the skills and knowledge necessary to help you investigate what may have happened on your computer and secure and protect your information.**

#1 - Self Assessment:

Answer the following questions:

1. What is cybersecurity? Why do we need it?

Cyber Security is the process and prevention of cyber attacks. We need it so then our information doesn’t get stolen online, as well as preventing the potential of leaks of that information.

1. Who does cybersecurity affect?

Everyone on the internet as well as everyone who uses computers.

1. What are some careers that relate to cybersecurity?

Information security analyst, Penetration tester, IT Security Engineer.

1. What is spam email?

Repetitive and unwanted emails typically from unknown sources.

1. What is phishing?  
   Phishing is emails sent in the form of some familiar or well known retailer, but the intention behind the message is to steal information from the recipient.
2. What is social engineering and what is its purpose?

Social engineering is the practice of manipulating people in order to give personal information.

1. What is malware?

Software designed to gain information or access to a computer without the user’s consent.

1. How can you ensure your browsing experience is secure? (Include web browser security features, as well as any security considerations related to the website you are visiting.)

Check the URL to make sure it’s secure, using a VPN is always a good idea, as well as making sure you’re not going into suspicious websites or clicking on any link you see.

1. What are the main components in a network?

Physical connections, Network Operating Systems, Application components.

1. How do you keep your computer safe from malicious content, such as unsafe files and harmful processes?

One easy way to keep your computer safe from malicious content is to download antivirus software. As well as overall being mindful about what you’re downloading and what files you’re using on your computer.

#2 - Use the information from the video to answer the following questions:

1. How did the internet become the cyberspace that we know today?
2. What are some examples of cybersecurity breaches?

# 4 - Digital Footprint - Google Drawing

# 5 - Notebook

# 6 - Notebook

#7 - Notebook

#9 - Notebook

Conclusion Questions - Notebook

* Reflect on your own cyber behavior. How does it compare to the Code of Conduct you just created? Explain.
* Where in the Cybersecurity Lifecycle does your inventory of personal data belong? What should be your next steps (or stages)?

**Unit 1.1.2**

**Please allow for 3 to 5 minutes before the lab opens**

**Goals**

* Protect your personal computer.
* Differentiate between a strong and weak password.
* Examine password cracking algorithms used in brute force attacks.
* Learn how authentication protects you online.

#4 - Notebook

#12 - Notebook & Screenshot

(Use TAB to make more rows from the last cell on the right)

|  |  |  |  |
| --- | --- | --- | --- |
| **Algorithm** | **Password** | **Guesses** | **Time** |
| **Crack One-Word** | **Hey** | **21387** | **0.00438439** |
| **Crack One-Word** | **Apple** | **21387** | **0.00446713** |
|  |  |  |  |

##13 - Notebook & Screenshot

|  |  |  |  |
| --- | --- | --- | --- |
| **Algorithm** | **Password** | **Guesses** | **Time** |
| 1: Crack one-word | hello | 8798 | .00159271 |
| **Crack Word-Symbol** | **Hello?** | **128322** | **.03702486** |
| **Crack Word-Symbol** | **Hello%** | **128322** | **.03113558** |

#14 - Notebook & Screenshot

|  |  |  |  |
| --- | --- | --- | --- |
| **Algorithm** | **Password** | **Guesses** | **Time** |
| 1: Crack one-word | hello | 8798 | .00159271 |
| 1: Crack one-word (beginning) | ... | ... | ... |
| 1: Crack one-word (end) | ... | ... | ... |
| 2: Average time one-word | ... | ... | ... |

#15 Notebook & Screenshot

|  |  |  |  |
| --- | --- | --- | --- |
| **Algorithm** | **Password** | **Guesses** | **Time** |
| 2: Crack one-word and symbol | ... | ... | ... |
| **Crack one word symbol** | **hello>** | **509179** | **0.17591809** |
| **Crack one word symbol** |  |  |  |

#21 - Notebook

#22 Notebook

#23 - Notebook

#24 - Screenshot

CAPTCHAS - Notebook

Conclusion Questions

* Reflect on the purposes of authorization and authentication and the roles they play in the Cybersecurity Lifecycle shown in Figure 5.
  + In which part of the Cybersecurity Lifecycle would you place authorization and authentication?
* Using a tool such as the password cracking algorithm to discover someone else’s password is almost always ethically wrong and in most cases illegal. Describe what you think an ethical use of the tool might be.

**Unit 1.1.3**

**Goals**

* Identify unsafe practices related to social media and email.
* Protect your social media profile.
* Protect against spam and phishing.
* Learn to evaluate suspicious email or websites.
* Learn how to protect against social engineering attacks.

#3 - Notebook

#4 - Notebook

#6 - Code of Conduct - Notebook

#8 - Notebook

#14 - Notebook

#15 - Notebook

#16 - Notebook

20-24 - Notebook & Screenshot of completed Matrix

Conclusion Questions:

* What are some data you identified in this activity that you need to protect?
* What are some considerations you can take to protect the identified data?

**Unit 1.1.4**

**Goals**

* Collaborate to create team norms as part of a cyber team.
* Create a list of recommendations to help co-workers.
* Role play as members of a help desk team and as co-workers with security concerns.
* Reflect on your collaborative experience with your cyber team.

**Project 1.1.4 Save the Day Rubric**

|  |  |  |  |
| --- | --- | --- | --- |
| Criteria | Basic | Proficient | Advanced |
| Risk Detection  LO 5.2: Identify personal data sharing that places people at risk and evaluate risky personal data-sharing practices. | The student identified no more than a **few** characteristics of suspicious emails. | The student identified **most** characteristics of suspicious emails. | The student identified **all** characteristics of suspicious emails. |
| The student identified no more than a **few** characteristics of inappropriate or risky social media posts. | The student identified **most** characteristics of inappropriate or risky social media posts. | The student identified **all** characteristics of inappropriate or risky social media posts. |
| The student identified no more than a **few** of the secure account settings. | The student identified **most** of the secure account settings. | The student identified **all** of the secure account settings. |
| The student identified no more than a **few** of the characteristics of strong passwords. | The student identified **most** of the characteristics of strong passwords. | The student identified **all** of the characteristics of strong passwords. |
| Documentation  LO 15.2: Recognize documentation as an indispensable part of the security process. | The student provided **minimal to no** documentation or the documentation is unorganized or hard to follow. | The student provided **adequate** documentation which is clear and organized. | The student provided **thorough** documentation which has great clarity and organization. |
| Collaboration  LO 14.2: Collaborate effectively as part of a team. | The student is **inconsistently** engaged and **inadequately** contributes to the team’s work. | The student is **consistently** engaged and **adequately** contributes to the team’s work. | The student is **consistently** engaged and **substantially** contributes to the team’s work. |
| The student **rarely** provides constructive feedback to others and **does not** encourage or incorporate input from others. | The student **occasionally** provides constructive feedback to others and **consistently** encourages and incorporates input from others. | The student **consistently** provides constructive feedback to others and **consistently** encourages and incorporates input from others. |

**Comments:**

**1.1.4 List**

# 3 Notebook

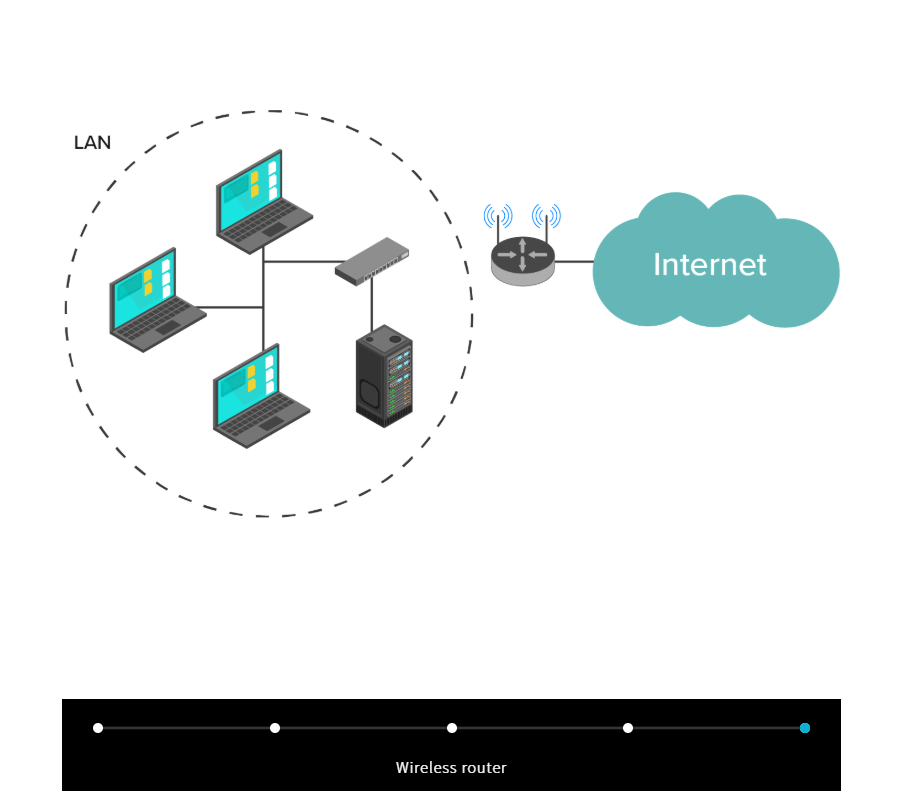
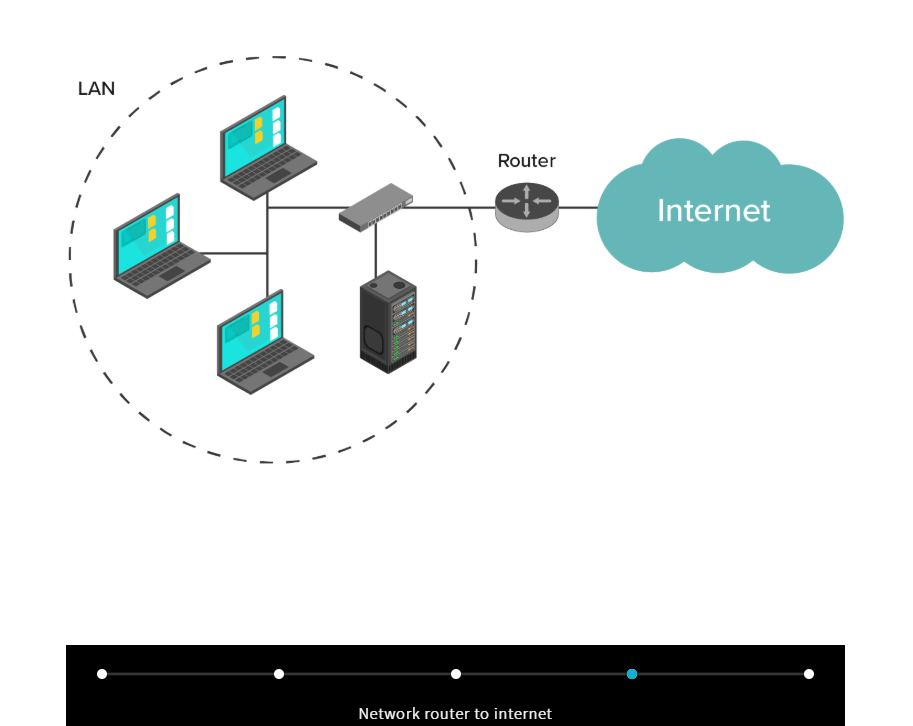
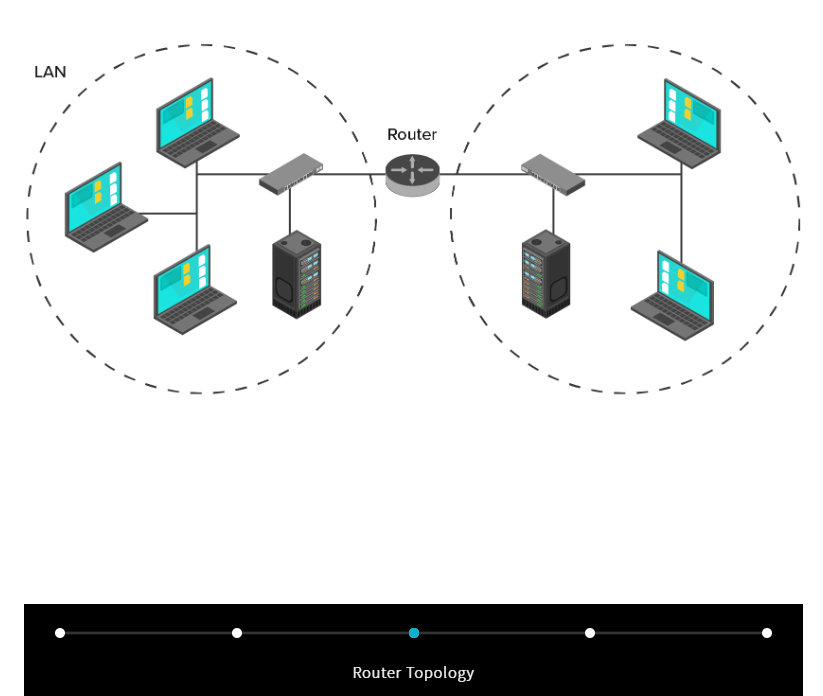
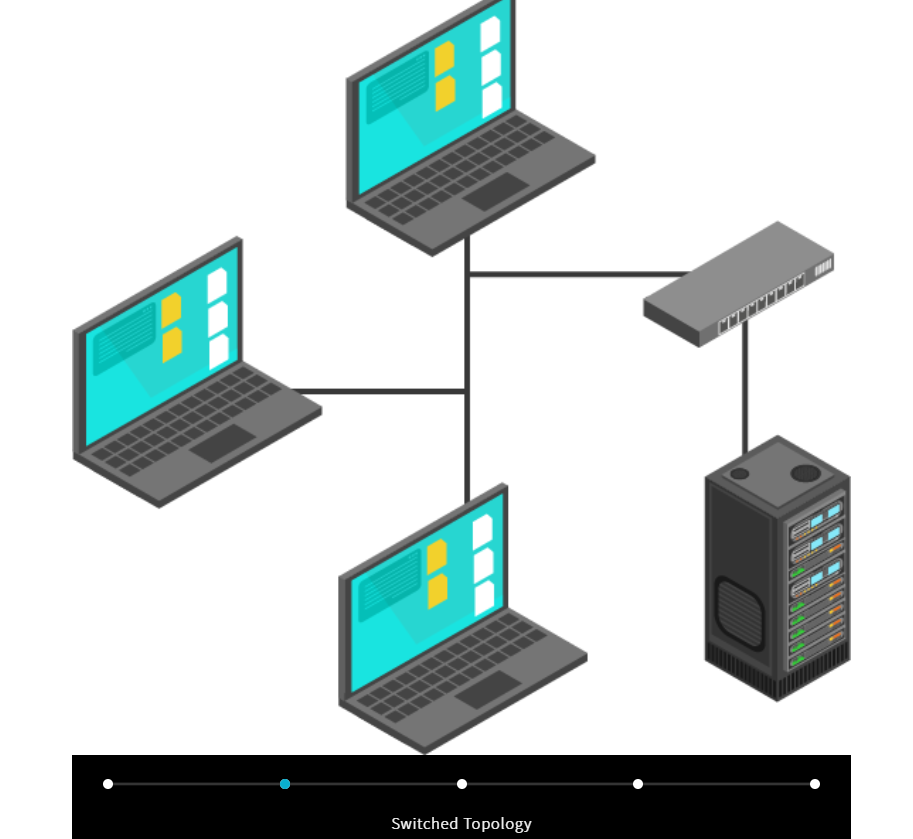
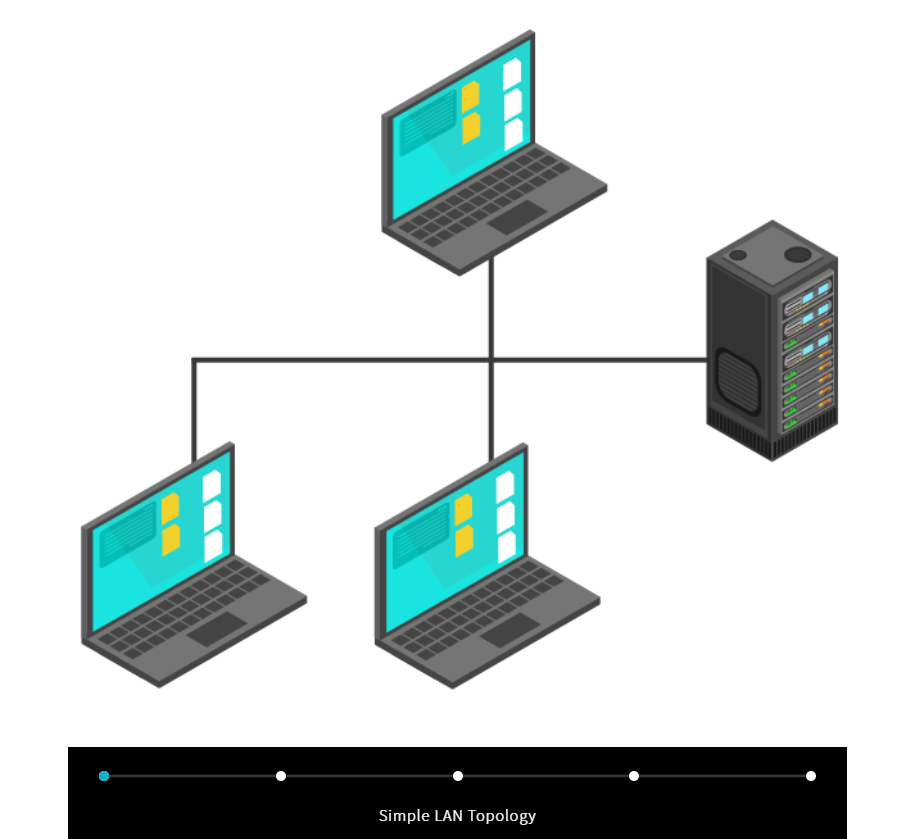
Computational Artifact - # 6 & 7

# 9 - Notebook

**Conclusion Questions**

* What are the pros and cons of elevating your social media privacy settings?
* Many employers review the social media accounts of job candidates. Should they use what they see on social media to influence hiring decisions? Why or why not?

**Unit 1.2.1**



**Goals**

* Learn how network devices are connected.
* Learn about types of malware.
* Configure a firewall to protect against malware.

**#2 Notebook**

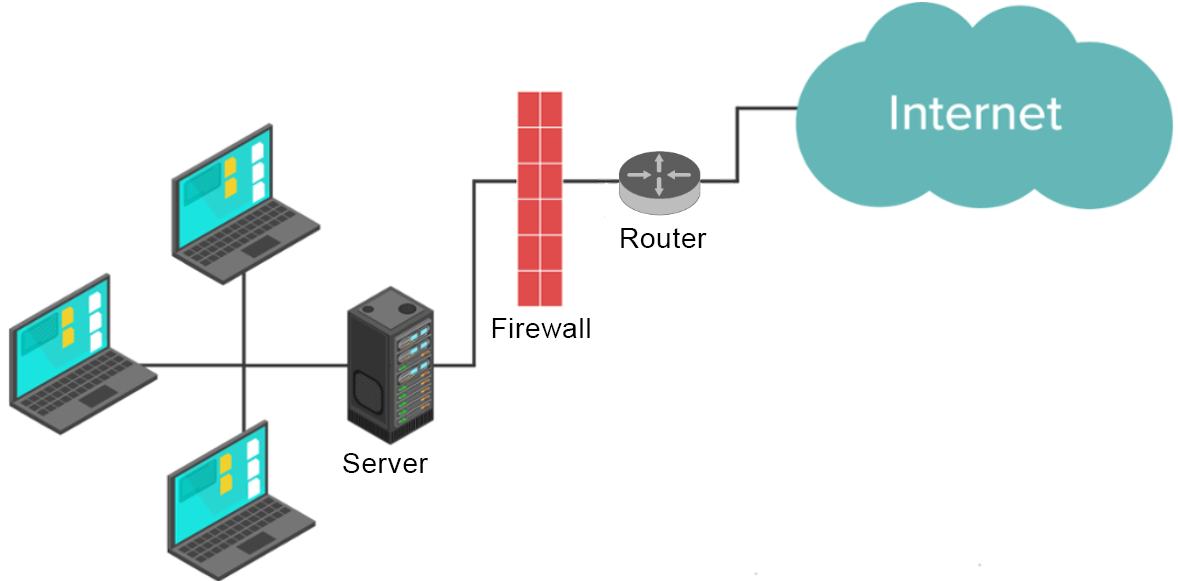
A Virus is malicious software that is spread by people or user actions, a worm is the same but doesn’t need user interaction to spread, a Backdoor bypasses secure and restricted access areas, Spyware is software that monitors and collects information about you, and a Trojan Horse is a program that is disguised as a safe program usually installed by the users.

**#7 Notebook**

Pop up ads, prompts such as entering personal info, sharing personal info/entering personal info into sites. You can avoid all this by not entering personal info, as well as not clicking on random links that lead to different areas.

**#15 Notebook**

Windows SmartScreen is a feature that helps prevent and block phishing and malware. It takes place every time it detects potential phishing or when you download a potentially harmful file.



**#23 Notebook & Screenshot**

**#26 Notebook & Screenshot**

**#31 Screenshot**

**#42 Notebook**

**Conclusion**

* Based on what you learned in this activity, what behavior changes might you make to reduce your personal risk in cyberspace?

**Encrypt all my data.**

**Unit 1.2.2**

**Goals**

* Learn about files and file types.
* Learn to access files safely and identify ownership
* Find hidden and files.
* Encrypt files.
* Learn to search files effectively.

#6 – Notebook

I was given a warning, I could've been hacked. It looks like a web page, but for the most part it's just a text document.

#7 – Notebook

It loaded the command terminal, it could've installed some malware, but nothing happened.

#8 – Notebook

One thing you can do to identify a file is to check it’s file type, another thing that can help identify a file is it’s display icon. By default the icon will correspond with the file type.

#10 – Notebook

.bat is a batch file, which consists of a series of commands to be executed at the command terminal, .doc is a document file created by Microsoft it’s basically a glorified text file that is compatible with document editors. .txt is a text file the only thing that’s really stored in a text file is just plain text.

#14 Screenshot

#20 – Notebook

Administrator

#21 – Notebook

Downloads, Image, Video, etc. Are all folders that are owned by the Administrator user.

#24 Screenshot

#27 - Notebook

A wildcard search is an advanced search method, it’s main purpose is to maximize the total number of search results within a library’s database.

#30 - Notebook

datemodified:today, datemodified:12/10/2021

#33 – Notebook

\*MyFile

#34 – Notebook

Listed files with the name of MyFile from multiple directories.

#35 - Screenshot

Conclusion Questions

* Discuss how each of the following items pose a threat to the security of a computer system:
  + - Opening a file
    - Hidden files/folders
    - File extensions
* For each of the items above, suggest one strategy to reduce the threat.

**Unit 1.2.3**

**Goals**

* Manage processes and the files that launched them.
* Recognize and terminate suspicious processes.

#9 – Notebook

D. AVG Technologies USA, Inc.

E. Yes, because it's from a reliable company.

#10 Notebook

Yes, because it's from a reliable company.

#14 – Screenshot

#22 - Screenshot

Conclusion Questions

* Discuss how file and process ownership can pose a threat to the security of a computer system.
* Suggest one strategy to reduce the threat.

**Unit 1.2.4**

**Goals**

* Manage browser configuration including security settings, cookies, history, downloads, and access to resources.
* Differentiate between HTTP and HTTPS
* Examine site certificates.

**#9 Notebook**

**Web Stores, Banks, Google, pretty much anything that is wanting information from the user. Including passwords, names, addresses, bank info, location access, etc.**

**#18 Notebook & Screenshot**

**#28 Notebook**

|  |  |
| --- | --- |
| **Not Saved or Visible** | **Saved and/or Visible** |
| **Browser History** | **Websites you visit** |
| **Cookies and site data** | **Your Employer or School** |
| **Information entered on forms** | **Your Internet service provider** |
|  |  |

**#37 Notebook & Screenshot**

**#41 Notebook**

**C:\Users\Administrator\Downloads\..**

**#43 Notebook**

**C:\Users\Administrator\Desktop**

**Conclusion Questions**

* What should you do if your computer is shared by your entire family and you install a plugin that saves usernames and passwords on the computer?
* How does having weak security on your browser represent the weakest link in a network?

**Unit 1.2.5**

**Goals**

* Collaborate with a cybersecurity team.
* Create and implement a plan of action.
* Reflect on your cyber team experience.

**Project 1.2.5 It’s A Trap! - Rubric**

|  |  |  |  |
| --- | --- | --- | --- |
| **Criteria** | **Basic** | **Proficient** | **Advanced** |
| **Risk Detection** LO 5.1 Find patterns and test hypotheses about digitally processed information to gain insight and knowledge.  LO9.1 Identify the components (software, hardware, protocols) that allow computers to network and communicate | The student identified **some** of the security issues related to:   * processes * downloaded files * other suspicious files * firewall rules | The student identified **most** of the security issues related to:   * processes * downloaded files * other suspicious files * firewall rules | The student identified **all** of the security issues related to:   * processes * downloaded files * other suspicious files * firewall rules |
| **Risk Protection** LO 8.1 Describe the modular components of a computer’s hardware and software.  LO 8.2 Identify user actions that strengthen the security of information stored on a computer. | The student identified no more than a **few** of the security configuration settings for:   * firewall rules | The student identified **most** of the security configuration settings for:   * firewall rules | The student secured **all** of the security configuration settings for:   * firewall rules |
| **Risk Response**  LO 10.3: Design the correct level of protection by implementing the appropriate safeguards. | The student removed no more than of a **few**   * suspicious processes and related application files * suspicious downloads * other suspicious files | The student removed **most** of   * suspicious processes and related application files * suspicious downloads * other suspicious files | The student removed **all**   * suspicious processes and related application files * suspicious downloads * other suspicious files |
| **Risk Recovery** LO 8.2 Identify user actions that strengthen the security of information stored on a computer. | *n/a* | *n/a* | The student recovered deleted data. |
| **Documentation**  LO 15.2: Recognize documentation as an indispensable part of the security process. | The student created **minimal to no** documentation explaining why the content poses risks and how it has been rectified. | The student created **adequate** documentation explaining why the content poses risks and how it has been rectified. | The student created **thorough** documentation explaining why the content poses risks and how it has been rectified. |
| **Collaboration**  LO 14.2: Collaborate effectively as part of a team.  LO 14.3 Apply project management strategies effectively as part of a team. | The student is **inconsistently** engaged and **inadequately** contributes to the team’s work. | The student is **consistently** engaged and **adequately** contributes to the team’s work. | The student is **consistently** engaged and **substantially** contributes to the team’s work. |
| The student **rarely** provides constructive feedback to others and **does not** encourage or incorporate input from others. | The student **occasionally** provides constructive feedback to others and **consistently** encourages and incorporates input from others. | The student **consistently** provides constructive feedback to others and **consistently** encourages and incorporates input from others. |
| **Presentation (Optional)**  LO 2.2 Engage stakeholder in a problem and use their perspectives to shape the course of your development.  LO 15.1: Communicate ideas, processes, and products to optimize audience perception and understanding. | The student **rarely** participates in the presentation. | The student **occasionally** participates in the presentation. | The student **substantially** participates in the presentation. |
| The presenter is **unclear,** presents **some** of the necessary information, and does **not** stay on topic. | The presenter is **clear,** presents most or **all** of the necessary information, but does **not** stay on topic. | The presenter is **clear,** presents **all** of the necessary information, and **stays** on topic. |
| The presenter **rarely** uses appropriate body language, voice modulation, and eye contact. | The presenter **occasionally** uses appropriate body language, voice modulation, and eye contact. | The presenter **consistently** uses appropriate body language, voice modulation, and eye contact. |

**Comments:**

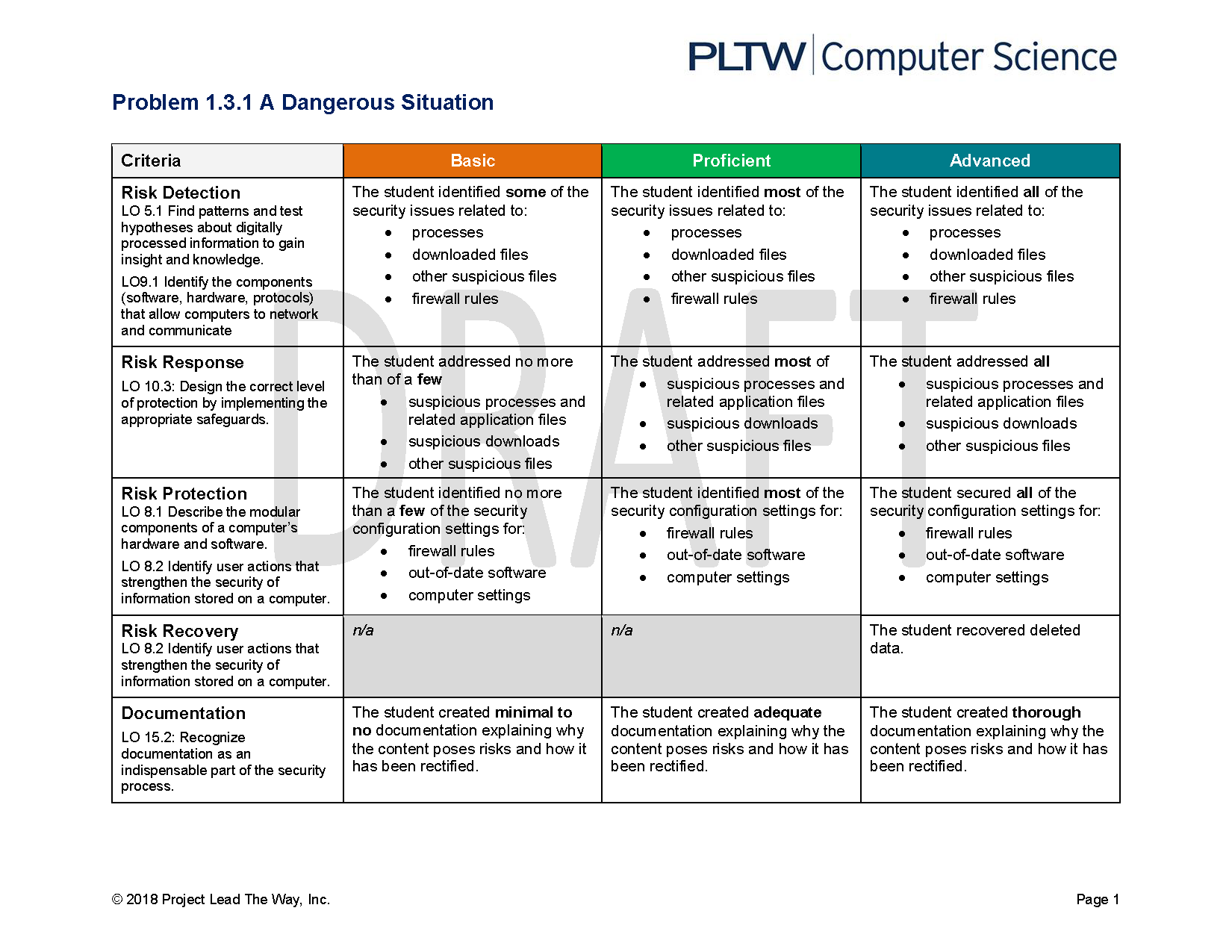
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Port Assignments for Well-Known Ports | | | |  |
| Port No. | Protocol | Service Name | Aliases | Comment |
| 7 | TCP | echo |  | Echo |
| 7 | UDP | echo |  | Echo |
| 9 | TCP | discard | sink null | Discard |
| 9 | UDP | discard | sink null | Discard |
| 13 | TCP | daytime |  | Daytime |
| 13 | UDP | daytime |  | Daytime |
| 17 | TCP | qotd | quote | Quote of the day |
| 17 | UDP | qotd | quote | Quote of the day |
| 19 | TCP | chargen | ttytst source | Character generator |
| 19 | UDP | chargen | ttytst source | Character generator |
| 20 | TCP | ftp-data |  | File Transfer |
| 21 | TCP | ftp |  | FTP Control |
| 23 | TCP | telnet |  | Telnet |
| 25 | TCP | smtp | mail | Simple Mail Transfer |
| 37 | TCP | time |  | Time |
| 37 | UDP | time |  | Time |
| 39 | UDP | rlp | resource | Resource Location Protocol |
| 42 | TCP | nameserver | name | Host Name Server |
| 42 | UDP | nameserver | name | Host Name Server |
| 43 | TCP | nicname | whois | Who Is |
| 53 | TCP | domain |  | Domain Name |
| 53 | UDP | domain |  | Domain Name Server |
| 67 | UDP | bootps | dhcps | Bootstrap Protocol Server |
| 68 | UDP | bootpc | dhcpc | Bootstrap Protocol Client |
| 69 | UDP | tftp |  | Trivial File Transfer |
| 70 | TCP | gopher |  | Gopher |
| 79 | TCP | finger |  | Finger |
| 80 | TCP | http | www, http | World Wide Web |
| 88 | TCP | kerberos | krb5 | Kerberos |
| 88 | UDP | kerberos | krb5 | Kerberos |
| 101 | TCP | hostname | hostnames | NIC Host Name Server |
| 102 | TCP | iso-tsap |  | ISO-TSAP Class 0 |
| 107 | TCP | rtelnet |  | Remote Telnet Service |
| 109 | TCP | pop2 | postoffice | Post Office Protocol - Version 2 |
| 110 | TCP | pop3 | postoffice | Post Office Protocol - Version 3 |
| 111 | TCP | sunrpc | rpcbind portmap | SUN Remote Procedure Call |
| 111 | UDP | sunrpc | rpcbind portmap | SUN Remote Procedure Call |
| 113 | TCP | auth | ident tap | Authentication Sevice |
| 117 | TCP | uucp-path |  | UUCP Path Service |
| 119 | TCP | nntp | usenet | Network News Transfer Protocol |
| 123 | UDP | ntp |  | Network Time Protocol |
| 135 | TCP | epmap | loc-srv | DCE endpoint resolution |
| 135 | UDP | epmap | loc-srv | DCE endpoint resolution |
| 137 | TCP | netbios-ns | nbname | NETBIOS Name Service |
| 137 | UDP | netbios-ns | nbname | NETBIOS Name Service |
| 138 | UDP | netbios-dgm | nbdatagram | NETBIOS Datagram Service |
| 139 | TCP | netbios-ssn | nbsession | NETBIOS Session Service |
| 143 | TCP | imap | imap4 | Internet Message Access Protocol |
| 158 | TCP | pcmail-srv | repository | PC Mail Server |
| 161 | UDP | snmp | snmp | SNMP |
| 162 | UDP | snmptrap | snmp-trap | SNMP TRAP |
| 170 | TCP | print-srv |  | Network PostScript |
| 179 | TCP | bgp |  | Border Gateway Protocol |
| 194 | TCP | irc |  | Internet Relay Chat Protocol |
| 213 | UDP | ipx |  | IPX over IP |
| 389 | TCP | ldap |  | Lightweight Directory Access Protocol |
| 443 | TCP | https | MCom |  |
| 443 | UDP | https | MCom |  |
| 445 | TCP | smb |  | Microsoft CIFS |
| 445 | UDP | smb |  | Microsoft CIFS |
| 464 | TCP | kpasswd |  | Kerberos (v5) |
| 464 | UDP | kpasswd |  | Kerberos (v5) |
| 500 | UDP | isakmp | ike | Internet Key Exchange (IPSec) |
| 512 | TCP | exec |  | Remote Process Execution |
| 512 | UDP | biff | comsat | Notifies users of new mail |
| 513 | TCP | login |  | Remote Login |
| 513 | UDP | who | whod | Database of who's logged on, average load |
| 514 | TCP | cmd | shell | Automatic Authentication |
| 514 | UDP | syslog |  |  |
| 515 | TCP | printer | spooler | Listens for incoming connections |
| 517 | UDP | talk |  | Establishes TCP Connection |
| 518 | UDP | ntalk |  |  |
| 520 | TCP | efs |  | Extended File Name Server |
| 520 | UDP | router | router routed | RIPv.1, RIPv.2 |
| 525 | UDP | timed | timeserver | Timeserver |
| 526 | TCP | tempo | newdate | Newdate |
| 530 | TCP,UDP | courier | rpc | RPC |
| 531 | TCP | conference | chat | IRC Chat |
| 532 | TCP | netnews | readnews | Readnews |
| 533 | UDP | netwall |  | For emergency broadcasts |
| 540 | TCP | uucp | uucpd | Uucpd |
| 543 | TCP | klogin |  | Kerberos login |
| 544 | TCP | kshell | krcmd | Kerberos remote shell |
| 550 | UDP | new-rwho | new-who | New-who |
| 556 | TCP | remotefs | rfs rfs\_server | Rfs Server |
| 560 | UDP | rmonitor | rmonitord | Rmonitor |
| 561 | UDP | monitor |  |  |
| 636 | TCP | ldaps | sldap | LDAP over TLS/SSL |
| 749 | TCP | kerberos-adm |  | Kerberos administration |
| 749 | UDP | kerberos-adm |  | Kerberos administration |

**#8 Notebook**

**#11 Notebook**

**#16 Notebook**

**Unit 1.3.1**



**#7 Notebook- Plan**

**#9 Notebook**

**#13 Notebook**

**Upload Incident report to this document**

**Conclusion Questions**

* While identifying your tasks in the Cybersecurity Lifecycle, some of your PROTECT tasks may have come after DETECT. Does this mean the task should be a RESPOND or RECOVER task? In general, how does the Cybersecurity Lifecycle represent an iterative approach to problem-solving?
* It turns out that two malicious users caused all of your security problems, and they were caught! One is a first-time offender and the other, a repeat offender; they are both students at your school. Describe the consequences that should be administered.