| Step 1: **Click** “File -> Make a Copy” to make a copy of this document that you can edit.    Step 2: **Change** the Share settings to “Anyone with Link -> Editor”. This will allow our graders to leave comments on your submission. |
| --- |

**CYB102 Prework (🔗** [**Instructions Page**](https://courses.codepath.org/snippets/cyb102/prework)**)**

👤 Student Name:

✉️ Student Email:

**Part 1: Bash-ing Your Way to Success (Required)**

*See the* ***🔗***[***Instructions Page***](https://courses.codepath.org/snippets/cyb102/prework) *for detailed instructions on completing Part 1. Once you’re done, come back here and add in your screenshot.*

| **Screenshot #1:** Your screenshot of Replit showing prework.sh and its’ output |
| --- |
| **[Insert Screenshot Here]** |
| **Notes** (Optional)**:** |

**Part 2: Thinking Like a Blue Teamer (Required)**

For this part, you’re going to be challenged to start thinking about computing from a blue team perspective. Don’t worry, there are no “right answers” to these questions – it’s just to get you thinking! Use your search engines and explore!

| **The Scenario** |
| --- |
| On a sunny afternoon, the employees of Happy Hippo Co., a small toy manufacturer, returned to their desks to find that they were unable to access any of their files. A message had popped up on their screens, demanding payment of 50 bitcoins, in exchange for the decryption key of their critical data that had been encrypted by a ransomware attack.  The message read, “Your files have been encrypted and are no longer accessible. Please follow the instructions below to obtain the decryption key. Payment must be made within 72 hours, or the decryption key will be permanently deleted.”  The IT team at Happy Hippo Co. quickly realized that their server had been attacked by ransomware, which had resulted in the encryption of critical data. The team tried to isolate the affected system, but it was too late, as the ransomware had already spread to all other systems on the network.  The CEO of Happy Hippo Co. contacted a friend, Bob the White Hat Hacker, who was a cybersecurity expert. Bob quickly analyzed the situation and provided a report stating that the ransomware attack was caused due to an employee clicking on a phishing email, which allowed the attacker to gain unauthorized access to the company’s network.  Bob also stated that the encryption used by the attacker was a strong one which used RSA-2048 encryption. He advised the company to not pay the attackers and instead to restore data from their backups.  The IT team quickly restored the data, which had been backed up regularly, and Happy Hippo Co. was back to business in no time. |

**Scenario Questions (Required)**

| **❓ Question #1:** What cybersecurity measures can Happy Hippo Co. implement to mitigate the risk of future ransomware attacks? (100+ words) |
| --- |
| [Identify assets that are searchable via online tools and take steps to reduce that exposure](https://www.cisa.gov/resources-tools/resources/stuff-search)  [Protecting Against Ransomware](https://www.cisa.gov/news-events/news/protecting-against-ransomware)  [Understanding Patches and Software Updates](https://www.cisa.gov/news-events/news/understanding-patches-and-software-updates)  [Using Caution with Email Attachments](https://www.cisa.gov/news-events/news/using-caution-email-attachments)  [SMB Security Best Practices](https://www.cisa.gov/news-events/alerts/2017/01/16/smb-security-best-practices)  [Website Security](https://www.cisa.gov/news-events/news/website-security)  [Rising Ransomware Threat to Operational Technology Assets](https://www.cisa.gov/resources-tools/resources/ransomware-threat-ot) |

| **❓ Question #2:** What policies and procedures should be put in place to educate the Happy Hippo Co. employees on the dangers of phishing emails? (100+ words) |
| --- |
| Never click any links or attachments in suspicious emails or Teams messages. If you receive a suspicious message from an organization and worry the message could be legitimate, go to your web browser and open a new tab. Then go to the organization's website from your own saved favorite, or via a web search. |

| **❓ Question #3:** How can an organization like Happy Hippo Co. quickly isolate systems that are affected to prevent the spread of ransomware attacks? (100+ words) |
| --- |
| Infections can be devastating to an individual or organization, and recovery can be a difficult process that may require the services of a reputable data recovery specialist.  US-CERT recommends that users and administrators take the following preventive measures to protect their computer networks from ransomware infection:   * Employ a data backup and recovery plan for all critical information. Perform and test regular backups to limit the impact of data or system loss and to expedite the recovery process. Note that network-connected backups can also be affected by ransomware; critical backups should be isolated from the network for optimum protection. * Keep your operating system and software up-to-date with the latest patches. Vulnerable applications and operating systems are the targets of most attacks. Ensuring these are patched with the latest updates greatly reduces the number of exploitable entry points available to an attacker. * Maintain up-to-date anti-virus software, and scan all software downloaded from the internet prior to executing. * Restrict users’ ability (permissions) to install and run unwanted software applications, and apply the principle of “Least Privilege” to all systems and services. Restricting these privileges may prevent malware from running or limit its capability to spread through the network. * Avoid enabling macros from email attachments. If a user opens the attachment and enables macros, embedded code will execute the malware on the machine. * Do not follow unsolicited Web links in emails. Refer to the [Phishing](https://security.berkeley.edu/resources/phishing) resources found on this website for more information.   Individuals or organizations are discouraged from paying the ransom, as this does not guarantee files will be released. However, the FBI has advised that if Cryptolocker, Cryptowall or other sophisticated forms of ransomware are involved, the victim may not be able to get their data back without paying a ransom. |

Nice job, that’s everything for the prework!

**Submission Checklist**

**👉***Check off each of the features you have completed.* ***You will only be graded on the features you check off.***

**Part 1: Challenge Screenshots**

* ~~Screenshot provided, showing:~~
  + ~~Contents of prework.sh~~
  + ~~Run output~~

**Part 2: Scenario Questions**

* ~~Question #1 answered above (100+ words)~~
* ~~Question #2 answered above (100+ words)~~
* ~~Question #3 answered above (100+ words)~~

**Submit your work!**

| Step 1: **Click** the Share button at the top of your screen double check that anyone with the link can edit. (This allows our grading team to input your grade below!)  <https://replit.com/join/lziegofdng-sbiyyaaanass>  https://docs.google.com/document/d/1YOTHicXoF9DLp9llhpbW2mb\_cIcIhLggnA\_ZFmRMj88/edit?usp=sharing    Step 2: **Copy** the link to this document.  <https://replit.com/join/lziegofdng-sbiyyaaanass>  https://docs.google.com/document/d/1YOTHicXoF9DLp9llhpbW2mb\_cIcIhLggnA\_ZFmRMj88/edit?usp=sharing  Step 3: **Submit** the link on the portal. |
| --- |

**Grader Comments**

| **Grading Rubric**  | Part 1: Challenge Screenshots | Total Received | Total Possible | | --- | --- | --- | | Prework.sh code is shown in screenshot |  | 2 | | Challenge #1 Passed |  | 2 | | Challenge #2 Passed |  | 2 | | Challenge #3 Passed |  | 2 | | **PART 1 TOTAL** |  | **8** | | Part 2: Scenario Questions | Total Received | Total Possible | | Question #1 answered above |  | 4 | | Question #2 answered above |  | 4 | | Question #3 answered above |  | 4 | | **PART 2 TOTAL** |  | **12** | | **Total Possible Points (Part 1 + Part 2)** |  | **20** | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |