6. A network monitor records the information below while recording a network connection. For each type of information collected, list any type of sanitize needed to conceal potentially confidential information, including user names, IP addresses, passwords, credentials, etc.

a. Process names including command line arguments
    a. A pseudonym is needed to hide the UID for which the process is being run under. For example if the UID is “Shane Cincotta”, it may be sanitized to become “User: 1”.
    b. Run time is also included in the process list (ps -ef), this can be sanitized as well by masking the time a process was run at.
    c. The command which is related to a process is also included with ps -ef, masking this can prevent a person from knowing which commands lead to which process running.
b. System control files such as the password file
    a. The password will need a filter with some type of encryption to make sure the passwords are not available in plaintext form.
    b. The usernames associated with the passwords will also need to be masked/encrypted.
    c. The access permissions of each user associated with each password will need to be masked as well, so one cannot see what commands/access level each user/password combo has.
c. A file containing a list of dictionary words
    a. If any of the words are classified for some reason (maybe the words correspond to an unreleased project) then the words themselves will need to be sanitized.
    b. The ACL should be sanitized to hide who can modify the file and to what degree
    c. The dictionary properties (type, size, parent folder, etc) might need to be sanitized. If this information is available, then the content of the dictionary might be deciphered.
d. A source code file
    a. Either all the content in the file should be sanitized or specific segments. It’s possible that the source code contains sensitive information
    b. The ACL should be sanitized to hide who can modify the file and to what degree
    c. The type of file might need to be sanitized. For example we might want to hide the fact that it’s a python or C file.
    d. The parent directory might need to be sanitized, the location of a source code file could reveal what function it serves and thus what kind of code it contains.
e. A Web page downloaded from a remote site
    a. The source HTML will need to be sanitized.
    b. The IP address and port number of the user who accessed it must be sanitized, as well as the host IP address and port number.
    c. Any usernames/passwords found in the HTML must be sanitized.
    d. The types of encryption used must be hidden
f. A Web server logs
    a. Hint: Go to google.com. Enter the text “Stephan Bohacek” Check the URL? Is there any PII in the URL? URLs are saved in the web server logs

    b. When I google the above text, I am able to see in the URL the OS I am using (Ubuntu) as well as the type of encoding I am using (UTF-8). Both of these pieces of information will need to be sanitized.

c. The IP address and port number of the user who accessed it must be sanitized, as well as the host IP address and port number.
d. Any usernames/passwords found in the log must be sanitized.
e. The types of encryption used must be hidden

Problem 2: Consider the security white paper here:
https://try.newrelic.com/rs/newrelic/images/New_Relic_Security_Whitepaper_2014_06.pdf

a. What is New Relic? Or service do they provide?
    a. New Relic is a venture capital company in CA. New Relic provides 24x7 real user monitoring and code-level diagnostics for web apps deployed on dedicated infrastructures, the cloud, or hybrid environments. They also provide their customers with instant visibility into the performance of deployed applications. New Relic helps protect your information from unauthorized access, use, or disclosure.
b. Where is the data stored?
    a. The data is stored in a Tier 3 SSAE 16 certified data center.
c. What types of compliance does New Relic have?
    a. Payment Card Industry Data Security Standard
    b. Health Insurance Portability and Accountability Act (HIPAA)
d. What options does New Relic have for collecting SQL queries? Why would one pick one option over the others
    a. SQL collection is configured by setting the record_sql parameter in the newrelic.yml file to one of the following three modes:
        i. off:
            1. New Relic does not collect or send any SQL code to the New Relic service.
        ii. obfuscated:
            1. New Relic collects SQL statements and replaces literal values in the “where” clause with obfuscated patterns. This is the default setting and provides a measure of security while still providing good visibility of the SQL queries in your application.
        iii. raw:
            1. New Relic collects and sends unaltered SQL statements to the New Relic service. By default, New Relic
    b. One would use the “raw” setting when no information needs to be sanitized.
    c. One would use obfuscation when there is information that needs to be sanitized.
    d. One would use off when no information should be sent either because it’s irrelevant or too sensitive.
e. If your database includes patient health records, what assurances can you give that the confidential data is secure.
    a. Using obfuscation will assure that sensitive data cannot be seen
    b. The HIPPA compliance will assure non-disclosure of protected health information (PHI).
    c. Access controls assure that only authorized users can access the information.
    d. User passwords are stored in an industry standard salted hash format.

e. New Relic’s servers are hosted in a world-class Tier 3 SSAE 16 certified datacenter in order to provide the highest level of security

Problem 4. Policy and auditing

a. How does policy relate to auditing?
    i. A cybersecurity policy sets the standards of behavior for activities. The goal of auditing is to detect any violation of a stated policy. Thus the records displayed in an audit will be directly related to the policies of a company. For example, if a company policy requires a specific username to identify who is accessing a file, that requirement will be shown when the audit is done to see who accessed that file. Thus the policies of a company are directly shown in the audit.

b. Gives one or more example of how policy impacts auditing?
    i. Since auditing is directly related to company policies, the information that is collected and reviewed in a log will show whether or not a policy was broken.
    ii. For example, if a policy requires a file to always remain on an in house server, an audit will show if that rule was actually followed, did the users adhere to the policy?
    iii. Policy also dictates what information is collected during an audit. For example, a company policy sets a requirement for the format of the usernames for all users on a system, but doesn’t dictate anything regarding the password format. Since there is no requirement for passwords, it doesn’t make sense to collect password information during the audit (as password formats aren’t part of this company policy), but we would want to collect information on the usernames since that is a company policy.

c. Does policy dictate all auditing?
    i. Not necessarily. It is possible that you want to audit/log information that is not directly a policy. The reason for this might be general security purposes. For example there might be a potential bug in the system at a company, you may want to log/audit information which may determine what/where the bug is, even though the reason for this log/audit was not explicitly said in company policy.

Problem 5: Consider a file server where a user is allowed to download files. Each file has an access control list (ACL) of the users that are allowed to download the file. The security policy is that only users listed in the access control list can download the file. **List the information that must be logged by a system that audits this policy.** Hint: Suppose the log says at 2020-03-12 12:34 Stephan makes a request to download file XYZ. Would this log information be suitable to determine if policy is enforced?

1. The ACL should be included.
    a. This will show if the privileges are as expected.
2. Information about attempted download of a file must be included.
    a. E.g if Shane Cincotta tries to download a file, the log should reflect that, regardless if I was able to successfully download it or not.
3. The access privileges of the user who tried to download the file should be included.
    a. E.g if Shane Cincotta tries to download a file, regardless if it was successful, what were that user’s privileges?
4. The success or failure should be included.

    a. E.g if a user tries to download a file, were they able to download it successfully?

5. This information is enough to determine if a company policy was followed. The general flow would look like the following:
    a. Who tried to access a file?
        i. What privileges does that person have?
    b. Were they successful?
        i. Given their privileges, should they have been able to access it according to the ACL?

Problem 6: Compare and contrast system logs and application logs

Contrast:

1. Application logging
    a. File of events that are logged by a software application
    b. Focuses on application events such as failure to make proper password
    c. Contains errors, informational events and warnings
    d. Focuses on the reasoning for an operation
    e. E.g web logs, database logs, email logs.
2. System logging
    a. A system log is a file containing events that are updated by the operating system components.It may contain information such as device drivers,events,operations or even device changes
    b. Focuses on system events such as memory mapping or file accesses.
    c. Focuses on the underlying cause.
    d. Larger than application logs (generally).
    e. E.g requesting memory, writing to standard output, starting processes, etc.

Compare:

1. Both indicate that something is wrong (E.g detecting violations of a known policy)
2. Both use some type of means to give details about “what” or “how” something went wrong.