Cybersecurity

Blue Yarrow Unicorns

Introduction

You were hired by the tech company Blue Yarrow Unicorns Inc. (Blue Yarrow) to conduct a cybersecurity penetration test (also called a pen test or ethical hacking) on the passwords used by its employees. Blue Yarrow provides digital consulting services to help companies manage new technologies. The company's name represents its desire to help companies solve challenging digital problems to be phenomenally successful. Blue represents the founder's favorite color and one that has inspired him. Yarrow is a traditional medicinal plant of healing. Unicorn represents the desire to help companies reach "unicorn" status — privately held companies with a valuation of over $1 billion.

Blue Yarrow works in diverse areas ranging from helping companies set up non-fungible tokens (NFTs) on blockchains to implementing drone solutions. For example, Blue Yarrow helped the agricultural companies Bryan's Amazing Animals Inc. (BAA) and Where's da Beef Inc. (WDB) build drone fleets to count their animals (see the EYARC *Innovation mindset* cases on these entities).

As a digital consulting company, many of Blue Yarrow's clients depend heavily on the solutions provided by Blue Yarrow for all aspects of their business. This reliance on Blue Yarrow's solutions means that many clients demand a Service Organization Controls (SOC) report from Blue Yarrow. Blue Yarrow has successfully achieved both a SOC 1 and a SOC 2 report in the past. The SOC 1 report provides an independent CPA's opinion about Blue Yarrow's internal control over financial reporting (ICFR) and the SOC 2 report provides an independent CPA's opinion about internal controls related to security, availability, processing integrity, confidentiality and privacy (for more information about SOC 1 and SOC 2 reports, see https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/serviceorganization-smanagement).

The SOC 2 report requires an auditor to evaluate the internal control monitoring activities of the company seeking the report. While this monitoring does not explicitly require penetration testing, it is recommended as a type of evaluation that auditors should consider performing. Since Blue Yarrow believes security is so important for their business, they have hired you to perform a pen test on password policies and practices.

Penetration tests can differ based on what the client wants. Blue Yarrow has defined this pen test to include the following:

- Blue Yarrow provided you with the file **Cybersecurity_case_studies_BlueYarrow_Unicorns_UserPasswords.xlsx**. The file contains two tabs of information.
  - On the tab "PasswordFile," the username and hashed password for each current employee are listed.
  - On the tab "User," the username, first name, last name and job unit of each current employees are listed.

SCORE no.15881-221US_3

- Blue Yarrow would like you to see how many passwords you can crack from this file, but Blue Yarrow does not want you to enter any usernames and passwords in their system. All of your work needs to be done in a tool outside of their system.
- Blue Yarrow would like you to provide a risk assessment and actionable recommendations based on your results. They are interested in recommendations based on what you observe in the data and any recommendations that you have after researching how to strengthen user security around system access and passwords.

One of your colleagues has already helped start preparing for the penetration test. She specifically highlights the following information for you:

- Blue Yarrow uses the MD5-Password hashing algorithm for all of their passwords. More specifically, they transcode the plain text password to UTF-8 before applying the MD5 algorithm. Blue Yarrow does not store plain text passwords.
- Blue Yarrow does not use password salts (unique random characters added to a password that is stored in a database with the password) or peppers (aka secret salt) (similar to a salt but not stored in a database with the password and not unique to each password). If you are interested in understanding more about salts or peppers, watch this brief video.
- Your colleague downloaded a list of common passwords that were discovered in prior internet leaks. The file is **Cybersecurity_case_studies_BlueYarrowUnicorns_PasswordDictionary.csv** and contains approximately 2 million common passwords. You should **not** search out other dictionaries on the web (especially since some of these lists can install viruses on your machine).
- In addition to the provided list, consider generating your own list of passwords to try — especially consider using any of the data provided as part of the list you create.
- Based on interviewing employees and reviewing system settings, it does not appear that Blue Yarrow enforces many standard password leading practices (e.g., see best practices by the Center for Internet Security (CIS) at https://www.cisecurity.org/white-papers/cis-password-policy-guide/). Keep this in mind as you perform your testing and make recommendations.
- There are 5,097 employees included in Blue Yarrow's files. We have confirmed there are no null passwords, and no employees are missing from the file.

Required

- Your task is to perform a cybersecurity penetration test of usernames and passwords. Your goal is to try and crack as many passwords as possible. C*omplete the requirements using Alteryx or Python as directed by your instructor.*
  - **Alteryx:** submit your completed workflows in a packaged Alteryx workbook (.yxzp file type [Options > Export Workflow >]) saved with a naming convention to include your full name, e.g., Cybersecurity_case_studies_BlueYarrowUnicorns_FirstName_LastName.yxzp. In addition, annotate each step in your workflow to indicate the purpose of that step. Also use comments to indicate the part of the workflow that answers each question posed.
  - **Python:** submit your completed code in a .py or .ipynb file (as directed by your instructor) saved with a naming convention to include your full name, e.g., Cybersecurity_case_studies_BlueYarrowUnicorns_FirstName_LastName.

SCORE no. 15881-221US_3

- You should then prepare and submit a memo that follows the format on the following page and with a naming convention to include your full name, e.g., Cybersecurity_case_studies_BlueYarrowUnicorns_FirstName_LastName.docx.
  - For your memo, remember that business readers value writing that is succinct, complete, accurate and specific.
  - Make certain to carefully proofread your results before submitting.

Memo format

To: Blue Yarrow Unicorn management and Board of Directors

Introduction

This section should be short and should describe the scope of your penetration test.

Methodology

This section should describe what you did to address Blue Yarrow's requests. Succinctly list all tests you conducted in this section. It is suggested you list each test in a bulleted list.

Results

This section needs to include the following table with the results of your testing.

Total users in the company file:		
Password cracking using the password dictionary		
Number of passwords cracked:		
Number of users with the same (i.e., repeated) cracked passwords:		
Number of passwords with the same (i.e., repeated) cracked passwords:		
The top 10 most repeated cracked passwords in plain text and the number of times each is repeated (in descending order):		
No.	**Plain text password**	**Number of times repeated**
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
Number of passwords not cracked:		
Number of users with the same (i.e., repeated) passwords not cracked:		
Number of the same (i.e., repeated) passwords not cracked:		

SCORE no. 15881-221US_3

Password cracking using own methods and not cracked using the password dictionary	
The number of passwords cracked:	
Description of the password cracking methodology and the number of passwords cracked (in descending order):	
Description of password cracking methodology	**Number of passwords cracked**
Use as many lines as appropriate	
Total number of cracked passwords *(sum of green fields above)*:	
Percentage of the total number of cracked passwords of the total of user passwords	

Risk analysis (quantitative and qualitative)

This section needs to include a risk analysis, both quantitative and qualitative, for Blue Yarrow based on the results.

Recommendations

This section needs to include recommendations for Blue Yarrow based on the risk analysis.