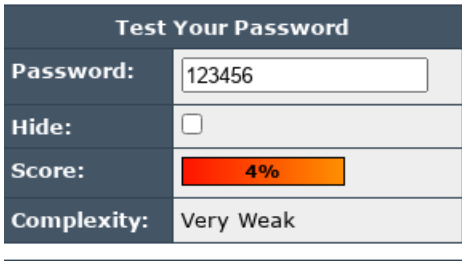
CYBR171 Cybersecurity Fundamentals
- Assignment 2: Social Engineering
- Due 11:59 pm Sunday 23th May 2021

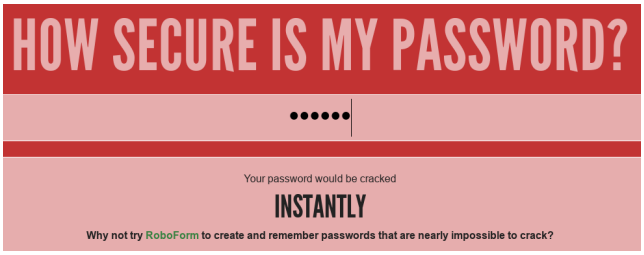
Please include the following in your assignment writeup:
- Assignment number, your full name and Student ID.
- Clearly labelled answers to the questions (Core 1, Challenge 99, etc).
- Report is submitted in electronic form as a txt or PDF file.

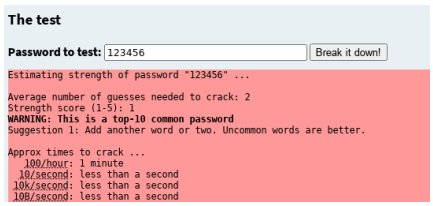
ASSIGNMENT NUMBER: 2
FULL NAME : Elisha Jones
STUDENT ID: 300573902

PART 1: Password Strength Meters
- Question 1.1

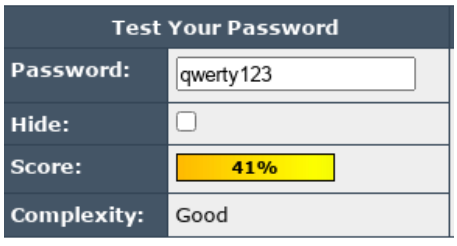
123456:

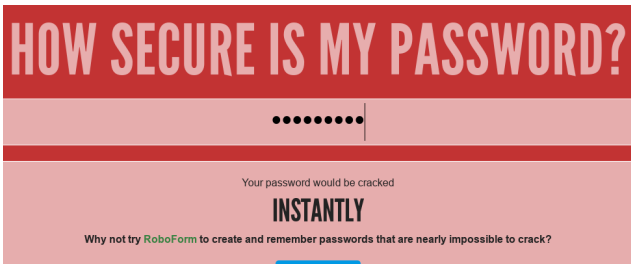


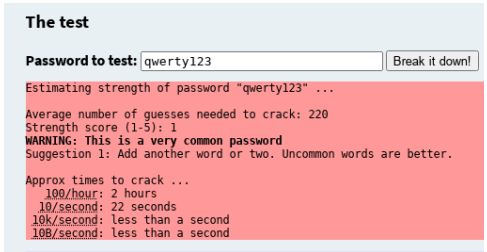




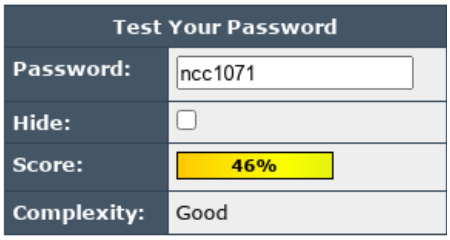
querty123:

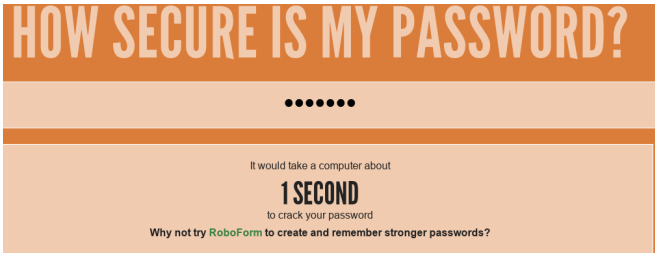


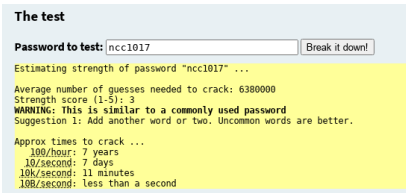




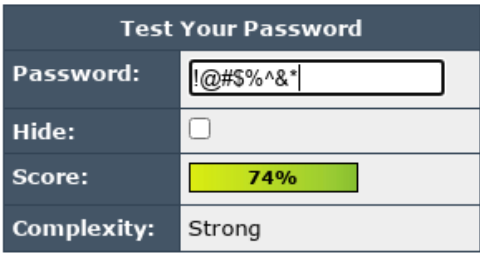
ncc1071:

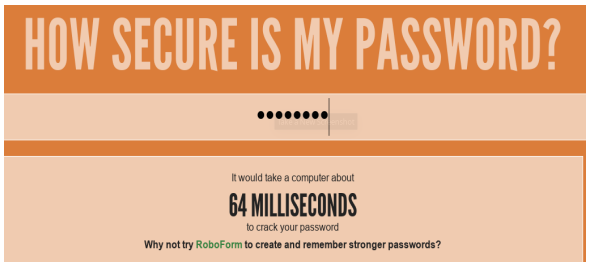


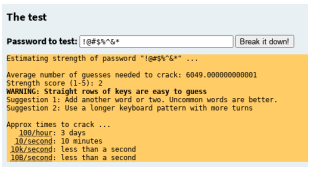




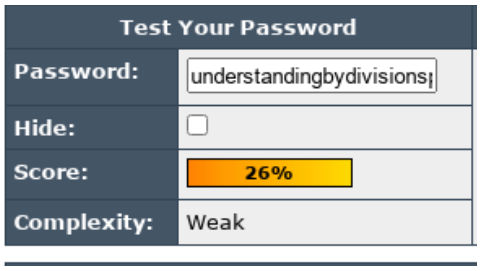
!@#$%^&*:

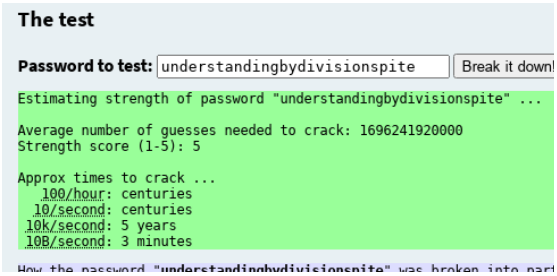






understandingbydivisionspite:



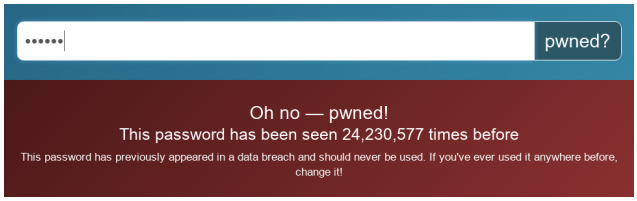


- Question 1.2

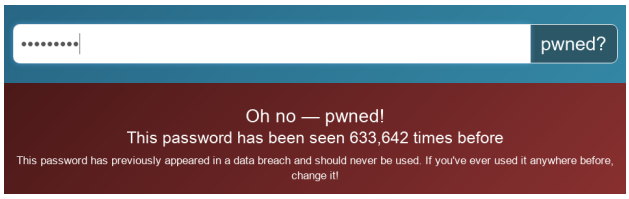
The best password is the fifth one (understandingbydivisionspite) was the best password for https://howsecureismypassword.net/ and https://www.bennish.net/password-strength-checker/. The 4th password (!@#$%^&*) was the strongest according to http://www.passwordmeter.com/

- Question 1.3

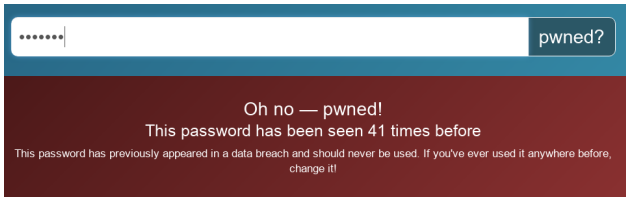
123456:



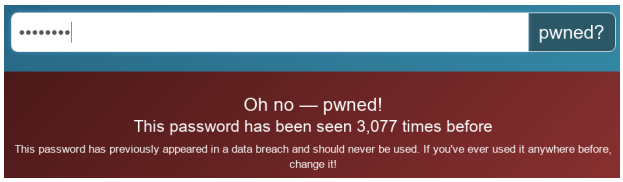
qwerty123:



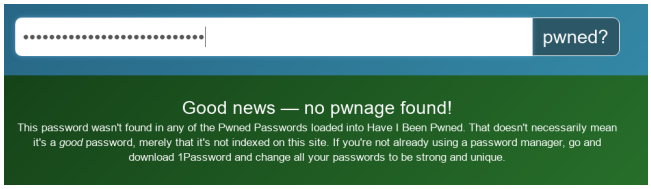
ncc1071:



!@#$%^&*:



understandingbydivisionspite:



- Question 1.4 [completion]

The best overall password seems to be understandingbydivisionspite as it is the most successful password in 3 quarters of the recorded tests.

- Question 1.5 [completion]

Based on the nature of the webpages, I'd imagine they have the entries compared across a database of confirmed hacked passwords and then compare the amount of times that the password has been hacked. If the password has never been hacked, the sites will register it as

safe. There is an associated risk in that the webpages may record what the user types and store it to the webpage, this could accidentally provide insight for a hacker to access accounts if they were able to somehow get the recorded entry. To minimise this risk, the password strength check has the page running through HTTPS and run through a javascript function so no actual information is sent to the server. The “have I been pwned” site only ever checks the first few keys of the hash and completely ignores the rest of the hash, to not store a full user password.

PART 2: Comparison of Secure Messaging

- Question 2.1

Telegram does offer end-to-end encryption for one-to-one chats but requires users to enable a "secret chats" feature, which must be switched on for every contact individually.

Signal uses encryption to the point where the Police would even be unable to get access to Signal messages.

Snapchat uses an end to end encryption for SNAPS ONLY and not individual messages

- Question 2.2

For increased protection from man in the middle attacks, all 3 apps have a multi-step authentication system that helps to increase the security of the accounts and prevent unwanted loggins on an individual's account. Most of these are done through mobile numbers which should only be accessible through the users mobile number. If you are using these apps to chat with another person that you know has a multi-step verification in place, there is very little risk of a man in the middle attack. Signal may be an only exception for this as Signal does support end-to-end encryption, but messaging people who do not have Signal installed will cause your messages to be unencrypted, as they are being sent outside the app. Telegram has relatively secure messaging as the official telegrams faq site states: “Client-Server communication is protected from MiTM-attacks during DH key generation by means of a server RSA public key embedded into client software. After that, if both clients trust the server software, the Secret Chats between them are protected by the server from MiTM attacks. The interface offers a way of comparing Secret Chat keys for users who do not trust the server” with the later option running just a user-user encryption with no servers involved.

- Question 2.3

Snapchat is particularly bad when it comes to trojans and is actually the source or one of the main spreaders of android trojans (Apple phones have no known security flaws that would allow a virus or a backdoor to be installed without being jailbroken). This can simply be done by creating a false third party app and submitting it to the app store or by sending a link to a site that auto downloads a trojan software. To add to this, if any of the apps are downloaded via the Apple app store, you can trust it is a verified app as only apps verified by apple can be added and downloaded from the app store. For signal, a link can be sent via the app to “ask a friend” to download the app, with no guarantee that a person has fabricated a fake link to install a trojan.

- Question 2.4 [completion]

In regards to secure communication I would use telegram as it appears to have the most secure user to user communication. Using a secret chat will also provide no possible way to decrypting any information given within the app without using a secret key (which can only be supplied via the user), and has no way of encrypting via the telegram servers as no information is stored on the telegram servers, meaning even if the servers are hacked, no information could be discerned regarding these secret conversations.

PART 3: Stealing the Examination

- Question 3.1

The academic staff (Aaron and Harith) and the programmers for attempt through the website. Whoever has the key for a locked file cabinet and in the Science Faculty office if going for physical copy (will be also harder) - not going to be referenced further.

- Question 3.2

For website attempt: the login information for one of the named people (username can be got via .vuw email which can be found on https://ecs.wgtn.ac.nz/Courses/CYBR171_2021T1/CourseOutline or https://www.wgtn.ac.nz/courses/cybr/171/2021/offering?crn=30039).

- Question 3.3

Steps:

- 1. Create a draft for phishing email that would require a logon for ecs in one way or another (ie. asking for marks) and create a redirect webpage.
- 2. Layout webpage like the ECS logon screen and have the submit button (for confirming password) redirect to the ecs homepage as well as send a message containing the logon information to yourself.
- 3. Finalise email and redirect site.
- 4. Send email to one or more of the supplied vuw emails
- 5. Await for a response and try login for anyone that falls for the phishing attempt.
- 6. If login works, navigate to the assignment page and get the copy.

- Question 3.4 [completion]

- I have used a phishing email as I believe it is the simplest to make look like an authentic question. As Well as this, I would be able to directly name the recipient of the email and avoid some of the red flags for phishing emails.

- Making a page that looks like the correct page it should be linking to is also a good part of phishing as it may help to build false trust that the page is an authentic page and not some trick.

PART 4: Online Marketplace Purchases

- Question 4.1

they put up multiple ads on websites like eBay, Cars.com, AutoTrader.com and CycleTrader.com with detailed advertisements for cars, motorcycles, boats and other high-value items generally priced in the $10,000 to $45,000 range (USD) for items that didn't actually exist.

After an agreement with the victim buyers, they would often email them invoices purporting to be from Amazon Payments, PayPal or other online payment services, with wire transfer instructions to try make themselves look official. Sometimes, the defendants allegedly pretended to sell cars from nonexistent auto dealerships in the United States and even created phony websites for these fictitious dealerships.

- Question 4.2 [completion]

Some manipulation was involved for some of the sales. One example of this is in the sale in which one of the scammers “allegedly pretended to be the widow of an Iraq war veteran who was selling her family’s mobile home so that she could care for her children” in order to get some sympathy from the potential “buyer”. They also used counterfeit service marks in designing their invoices so that they would appear identical to legitimate payment services like pay-pal or visa to appear official to ensure trust with the potential “buyers”.

- Question 4.3 [completion]

Precautions that should be mentioned:

1. Check the seller's past selling history and reviews from past buyers. - this can help provide information on how honest the seller is
2. Check emails provided that they should only be sent from proper payment services - self explanatory, make sure money is going through a trusted source.
3. Cross reference with existing store page for dealerships that are selling items online - can easily identify whether a car or other item actually exists.

PART 5: Password File Woes

Md5 hash of file 6ec3c38863adbe64a7442037728892b5

- Question 5.1 [challenge]
- Question 5.2 [challenge]
- Question 5.3 [challenge]
  1. I imported both keys using the command line and supplied passwords.
  2. Trusted the fingerprint for libr8
  3. Attempted to decrypt via “openssl enc -d -bf-cbc -in passwd.bf.enc.asc -out myfile.txt” with guessing the password: guesses (ardern, jacinda, mirrors, Mirrors,