HACK UTK

October 9th, 2018

Passwords and Phishing

https://hackutk.slack.com/

Human Passwords

- Tend to be pretty awful
  - I’m not trying to remember 15 chars
    - “binghamton1” - initial

Human Passwords

- Tend to be pretty awful
  - I’m not trying to remember 15 chars
    - “binghamton1” - initial
    - “**B**inghamton1” - upper case

Human Passwords

- Tend to be pretty awful
  - I’m not trying to remember 15 chars
    - “binghamton1” - initial
    - “**B**inghamton1” - upper case
    - “Binghamton1**!**”- special char

Human Passwords

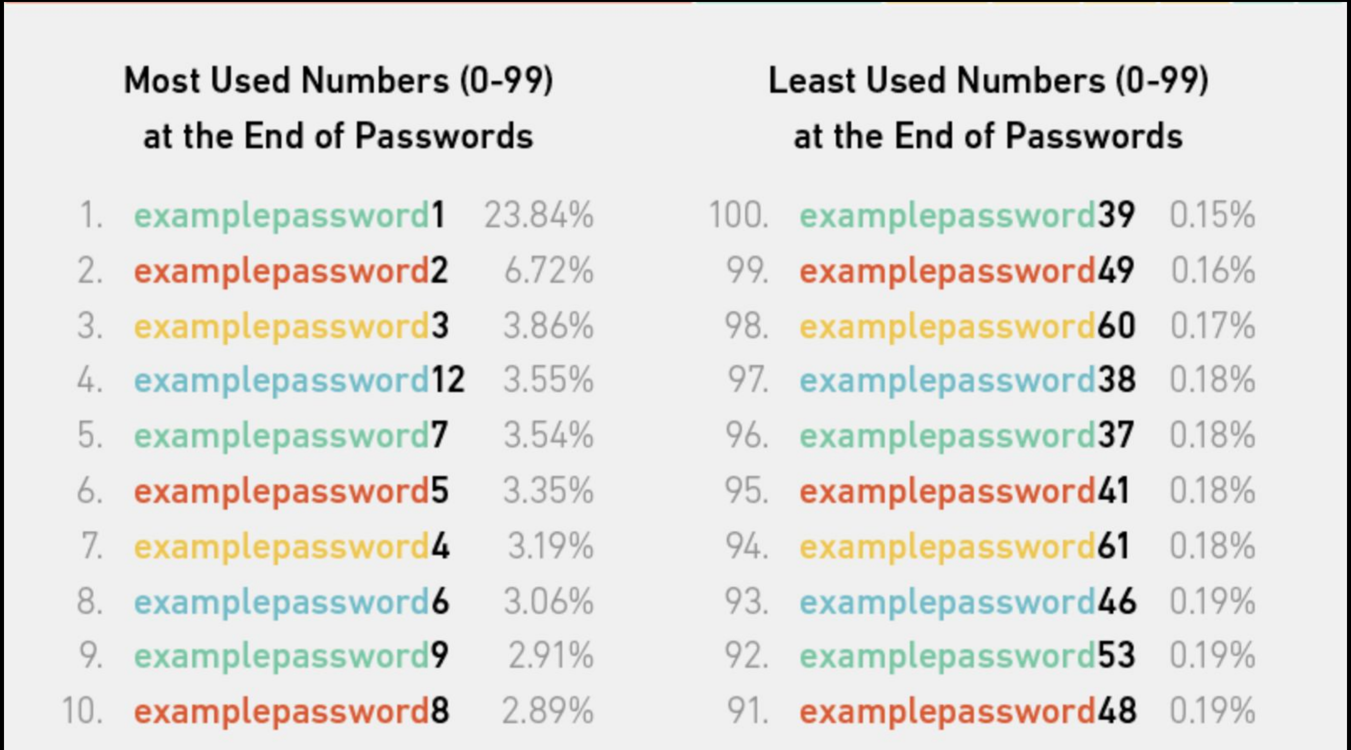
- Tend to be pretty awful
  - I’m not trying to remember 15 chars
    - “binghamton1” – initial
    - “**B**inghamton1” – upper case
    - “Binghamton1**!**”– special char
    - “Binghamton1**2**!” – can’t be same

Human Passwords

- https://wpengine.com/unmasked/

- Nearly half a million, or 420,000 (8.4 percent), of the 10 million passwords ended with a number between 0 and 99.

Human Passwords



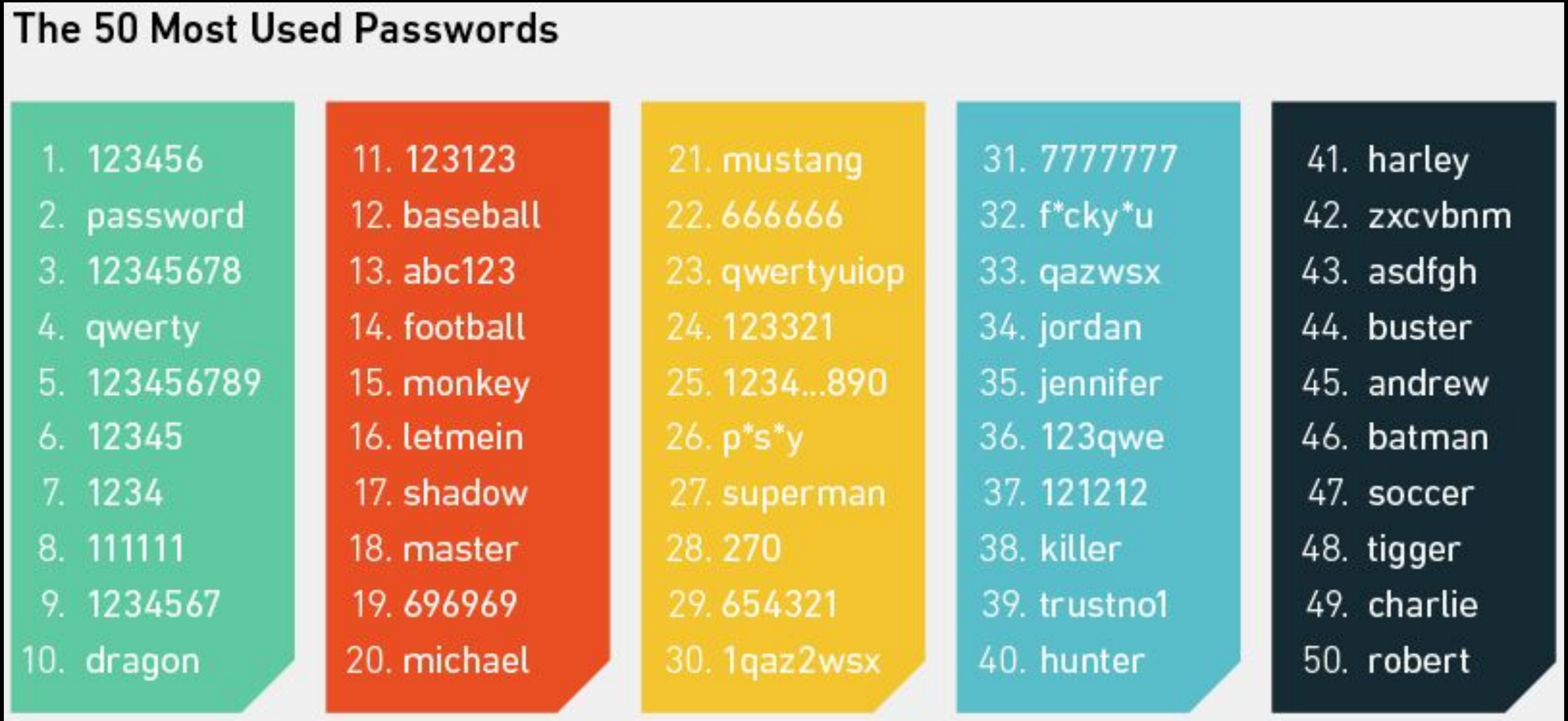
Most Used Numbers (0-99) at the End of Passwords

1.	examplepassword**1**	23.84%
2.	examplepassword**2**	6.72%
3.	examplepassword**3**	3.86%
4.	examplepassword**12**	3.55%
5.	examplepassword**7**	3.54%
6.	examplepassword**5**	3.35%
7.	examplepassword**4**	3.19%
8.	examplepassword**6**	3.06%
9.	examplepassword**9**	2.91%
10.	examplepassword**8**	2.89%

Least Used Numbers (0-99) at the End of Passwords

100.	examplepassword**39**	0.15%
99.	examplepassword**49**	0.16%
98.	examplepassword**60**	0.17%
97.	examplepassword**38**	0.18%
96.	examplepassword**37**	0.18%
95.	examplepassword**41**	0.18%
94.	examplepassword**61**	0.18%
93.	examplepassword**46**	0.19%
92.	examplepassword**53**	0.19%
91.	examplepassword**48**	0.19%

Human Passwords



The 50 Most Used Passwords

1. 123456
2. password
3. 12345678
4. qwerty
5. 123456789
6. 12345
7. 1234
8. 111111
9. 1234567
10. dragon
11. 123123
12. baseball
13. abc123
14. football
15. monkey
16. letmein
17. shadow
18. master
19. 696969
20. michael
21. mustang
22. 666666
23. qwertyuiop
24. 123321
25. 1234...890
26. p*s*y
27. superman
28. 270
29. 654321
30. 1qaz2wsx
31. 7777777
32. f*cky*u
33. qazwsx
34. jordan
35. jennifer
36. 123qwe
37. 121212
38. killer
39. trustno1
40. hunter
41. harley
42. zxcvbnm
43. asdfgh
44. buster
45. andrew
46. batman
47. soccer
48. tigger
49. charlie
50. robert

Dictionary Attacks

- Brute-force approach

- Try every password in a list of common passwords
  - Often called a dictionary
  - Where to find these dictionaries?
    - Online...

Password Storage

- Rarely ever stored in plain-text
  - If so, blow the whistle

- A **hash** of the password is stored

Hash Functions

- One-way and deterministic

Example – Deterministic

- Example:
  - Hash(“hello”) = 0xAAAAAAAA
  - Hash(“hello”) = 0xAAAAAAAA

Example - One Way

- Example:
  - Hash(“hello”) = 0xAAAAAAAA

Example - One Way

- Example:
  - Hash(“hello”) = 0xAAAAAAAA
  - Hash(0xAAAAAAAAA) = 0xABCD59DC

Hash Functions

- One-way and deterministic
- **Fixed size output**

Example – Fixed Size

- Example
  - Hash(“hello”) = 0xAAAAAAAA

Example – Fixed Size

- Example
  - Hash(“hello”) = 0xAAAAAAAA
  - Hash(“goodbye”) = 0xABCDEF12

Example - Fixed Size

- Example
  - Hash(“hello”) = 0xAAAAAAAA
  - Hash(“goodbye”) = 0xABCDEF12
  - Hash(“longgggggboi”) = 0xFEFEFEFE

All 8 chars (8*4 = **32bits**)

Hash Functions

- One-way and deterministic
- Fixed size output
- **Susceptible to collisions**

Example - Collisions

- Example
  - Hash(“hashme”) = **0xBBBBBBBB**

Example - Collisions

- Example
  - Hash(“hashme”) = 0xBBBBBBBB
  - Hash(“metoopls”) = 0xBBBBBBBB

Example - Collisions

- Example
  - Hash(“hashme”) = 0xBBBBBBBB
  - Hash(“metoopls”) = 0xBBBBBBBB

- Someone can login with a different password if it hashes to the same value

Example - Collisions

- Example
  - Hash(“hashme”) = 0xBBBBBBBB
  - Hash(“metoopls”) = 0xBBBBBBBB

- **Every hash function has collisions!!!**

Secure Hash Functions

- Susceptible to collisions

For **n** bit outputs, should roughly require **2^n** hashes to find a collision

Example - Collisions

- Example
  - Hash(“hello”) = 0xAAAAAAAA

All 8 chars (8*4 = **32bits**)

- Need to attempt **2^32** hashes to find a collision...

Example - Collisions

- Boils down to a for loop from
  - **0** to **~4 billion**
  - Not good enough...

- We want our **n** to be bigger

SHA256 Hash Function

- Output is 256 bits
  - 64 hex character string

SHA256 Hash Function

- Output is 256 bits
  - 64 hex character string
- Need to attempt 2^256 hashes to find a collision
  - This number is **exponentially** bigger than the number of atoms in the perceivable universe

Dictionaries for Hashes?

- Rainbow Tables
  - Precomputed tables matching hash values to potential passwords

Dictionaries for Hashes?

- Rainbow Tables
  - Precomputed table matching hash values to potential passwords
  - Essentially a way to determine a **plaintext** password from a **hash value**

Dictionaries for Hashes?

- Rainbow Tables
  - Precomputed table matching hash values to potential passwords
  - Essentially a way to determine a **plaintext** password from a **hash value**
  - Downside: can take terabytes of storage...

Rainbow Table

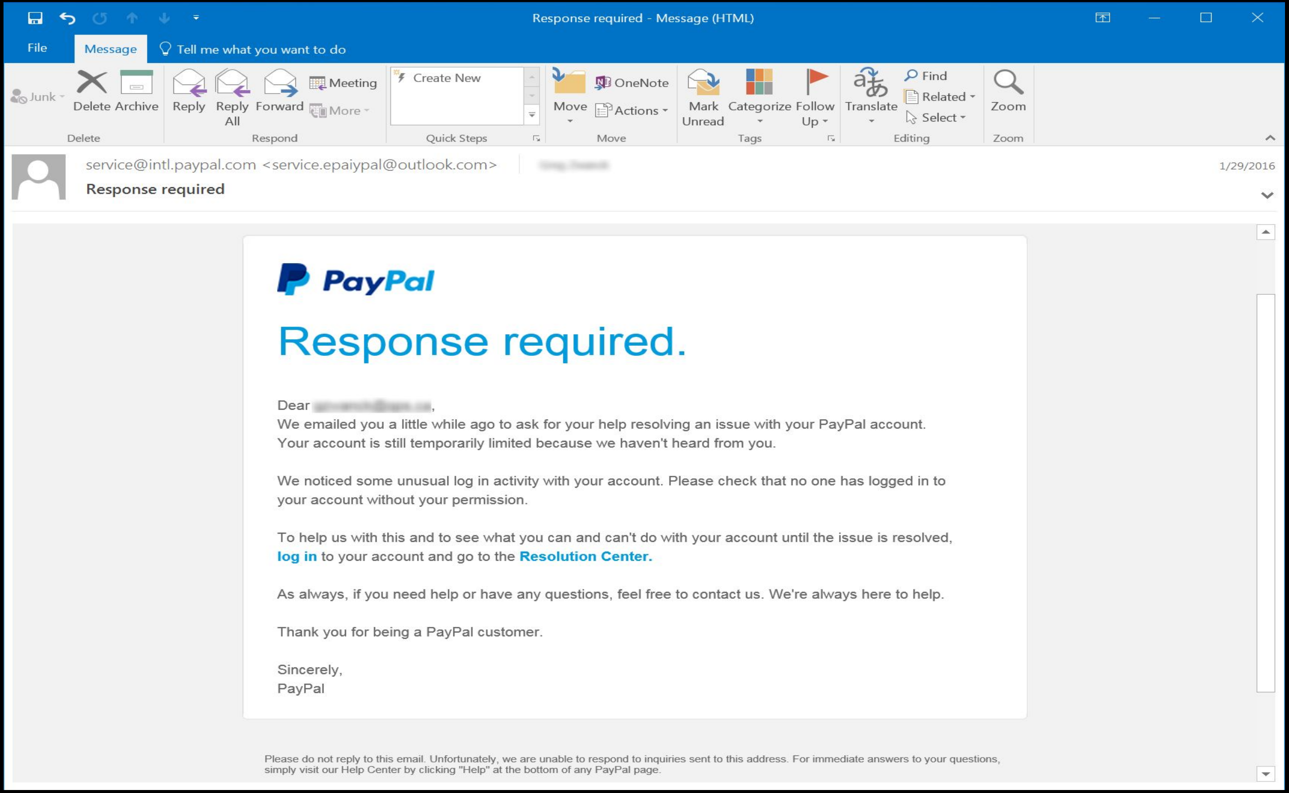
- Rainbow Tables
  - https://crackstation.net/
  - Not technically a Rainbow Table...

Phishing

- Instead of brute-forcing, why not just trick people into telling us their pw?

- Can be highly effective depending on target audience...

Phishing Examples



service@intl.paypal.com <service.epaiypal@outlook.com> [redacted]

1/29/2016

Response required

PayPal

Response required.

Dear [redacted],
We emailed you a little while ago to ask for your help resolving an issue with your PayPal account. Your account is still temporarily limited because we haven't heard from you.

We noticed some unusual log in activity with your account. Please check that no one has logged in to your account without your permission.

To help us with this and to see what you can and can't do with your account until the issue is resolved, **log in** to your account and go to the **Resolution Center.**

As always, if you need help or have any questions, feel free to contact us. We're always here to help.

Thank you for being a PayPal customer.

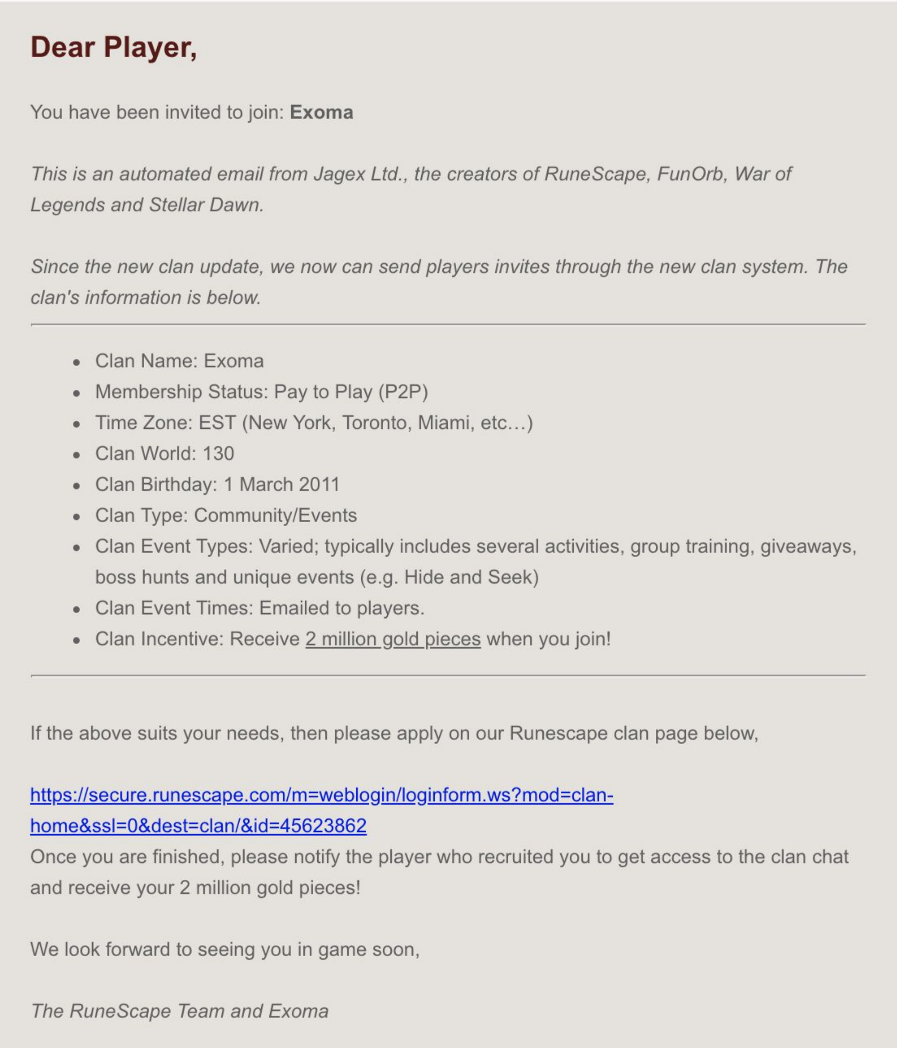
Sincerely,
PayPal

Please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking "Help" at the bottom of any PayPal page.

Personal History

- Loved me some Runescape at ~14 yrs old

- Fell for a phishing scam and came back with a vengeance...



Dear Player,

You have been invited to join: **Exoma**

This is an automated email from Jagex Ltd., the creators of RuneScape, FunOrb, War of Legends and Stellar Dawn.

Since the new clan update, we now can send players invites through the new clan system. The clan's information is below.

- Clan Name: Exoma
- Membership Status: Pay to Play (P2P)
- Time Zone: EST (New York, Toronto, Miami, etc…)
- Clan World: 130
- Clan Birthday: 1 March 2011
- Clan Type: Community/Events
- Clan Event Types: Varied; typically includes several activities, group training, giveaways, boss hunts and unique events (e.g. Hide and Seek)
- Clan Event Times: Emailed to players.
- Clan Incentive: Receive 2 million gold pieces when you join!

If the above suits your needs, then please apply on our Runescape clan page below,

https://secure.runescape.com/m=weblogin/loginform.ws?mod=clan-home&ssl=0&dest=clan/&id=45623862
Once you are finished, please notify the player who recruited you to get access to the clan chat and receive your 2 million gold pieces!

We look forward to seeing you in game soon,

The RuneScape Team and Exoma

Runescape

- That link redirected to:

http://services.**runescoqe**.com/m=clan-home/clan/exoma.ws?code=67ff69df471eb56edeae85346bc67f44&ssl=1&id=761509104543

Runescape

Don’t let a 14 year old steal your password!

Hashing Workshop

www.github.com/hackUTK/Fall2018

Workshop inside “Passwords Meeting” Folder