DEFENSE AGAINST THE DARK HATS

How to navigate the ever-changing landscape of attack and defense

Cryptography

- May refer to cryptography in general or to a specific family of ciphers that are related
- The **may** be **a** **family** **of** **ciphers** **that** **are** **used** to encode and decode messages, but **a** **key** **is** **required** to encode or decode

KEY

Cryptography Activity

- Identify the vulnerabilities in the website
- Use the Username: DATDH (for Defense Against the
- Guess the password!
- To decode each message, you can use the Caesar Cipher (which is the

Cryptography Activity

- Text Cipher Numbers
  - PICOCTF{ALLCAPSNOSPACES}
  - Apply a Caesar cipher
- Caesar Cipher
  - picoCTF{lowercasenospaces}
  - The answer is in the flag
- Easy 1 Cipher (Caesar cipher)
  - picoCTF{ALLCAPSNOSPACES}
  - Actually the easy HINT: the KEY letters, can be the
- 13 Cipher
  - picoCTF{lower_case_with_underscores}

Map i

THE HISTORY OF CRYPTOGRAPHY AND OF HACKING

HACKING AROUND THE WORLD

HOW TO BE A WHITE HAT

T h e Cy

- Nov 2, 1988 T gl b al cy e s cu e f i i y a ck s h
  bffer -w f w e x i t i n e a
  - Abt 10% f al c p d h e i n e w e d e e
- Tw n w defe s a e g i es e g ed f n h
  - Ty t d e e ct t i ed t a n -v h f e c e d if i i s w e) e s(s
  - B k al p ck s e x c p t h e s d el i v e d
- Rep s t f - i a e d t h e w s i ack s l i
  l eg i a ack a d e s t i n e w b s
- Rep s t a n -v s w e i - i c h s h ack s a g ed
  b e i d e n f t i i f

Man-in-the-Middle

- Points A and B think they are talking to each other
- Instead, SPY, SPY, is intercepting messages and forwarding them

ActOta Man- -t -M i h i

Cats **Joe Browser** (wstbw t h e i rfav i

Bette Midler (i tcept h e wbs i

Ender Wiggin (eg i t i ate wb s i

Exale d i alge:

Joe: H i Ender, h vae yo do i

Bette (i tcep i gt h e g

Ender (t h i k i gt gtay h i gsts h ybtf

Bette (toe): H i Joe, le gtay h .i

NOTE: Hae t h e aatels w h att h e pe pas

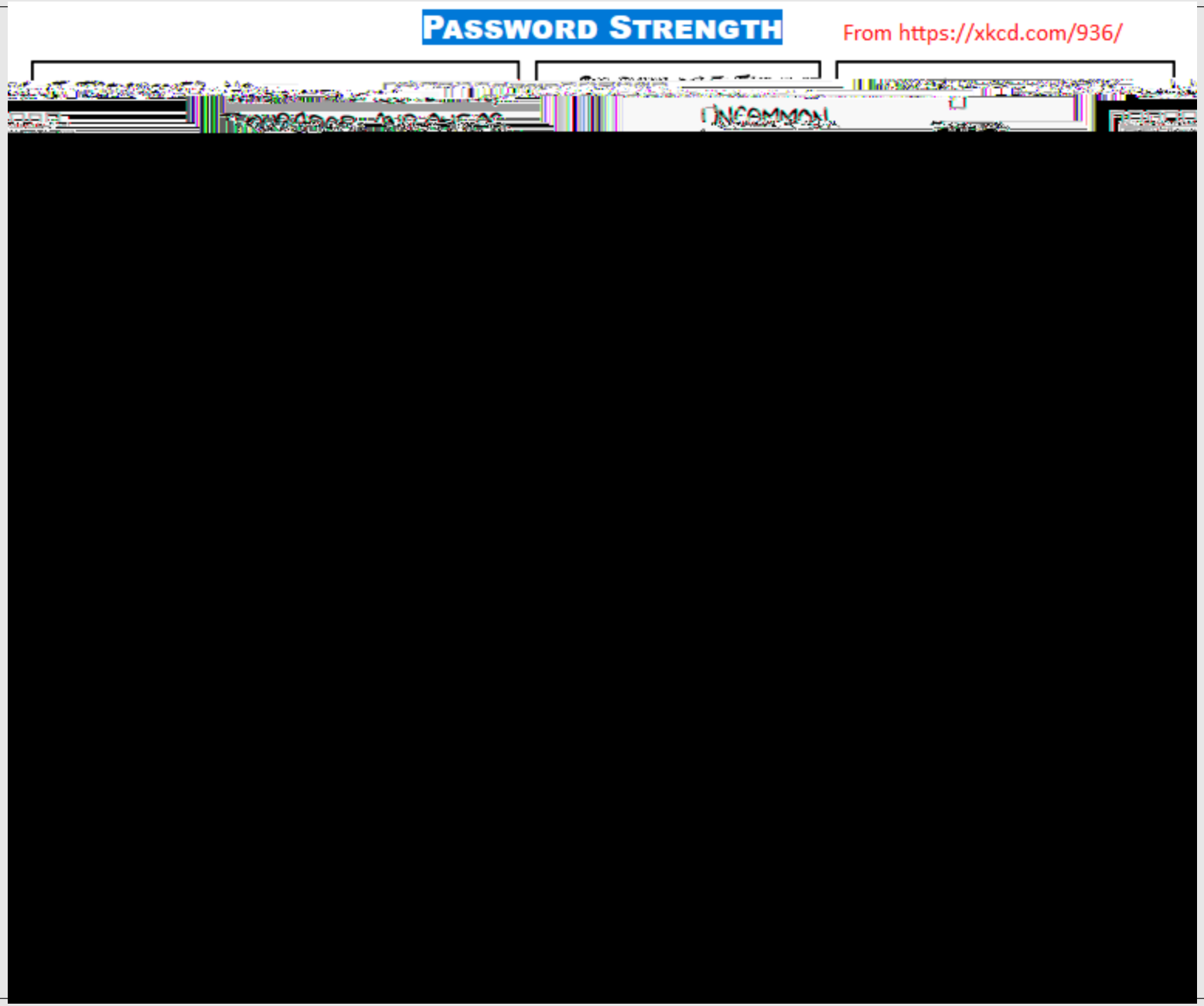
C h age t h e aes, tctt h - e

Cracking Passwords

- Passwords are used as keys to access:
  - Your GMail, Instagram, Snapchat, Twitter
  - Your Amazon and Ebay accounts
  - Your Facebook, Warcraft, Minecraft, League of Legends, etc.
- Passwords are often stored in encrypted form
  - But with enough computing power it is possible to find a match
  - When cracking passwords, hackers often exploit the fact that a cracked password is

PASSWORD STRENGTH

From https://xkcd.com/936/



Password Recommendations

- Use 12-character minimum
- Use passphrases, and maximize length
- Avoid dictionary words
- Don't use passwords from other sites
- Use a different password for each service
- Don't use repeated characters
- A good password is easy to remember, but hard to guess
  - Ow!1778SSE

Lo ra i ve Ca

- T h ee w i lbe as ay as 3.5 m i
- A y i calSecu i ty Se A dm i n
- A pe a t i de e **ethically** ac a ca y(ce s h e ca acta BEFOREHAND) t h en s h w h
  - Acc d Z i t i g h pecu e ave age Pe e s a y e i m 2021
- T h ee cy e secu i ty and IT bas d ex cu i

YOU MADE IT!

Let's play a game to celebrate