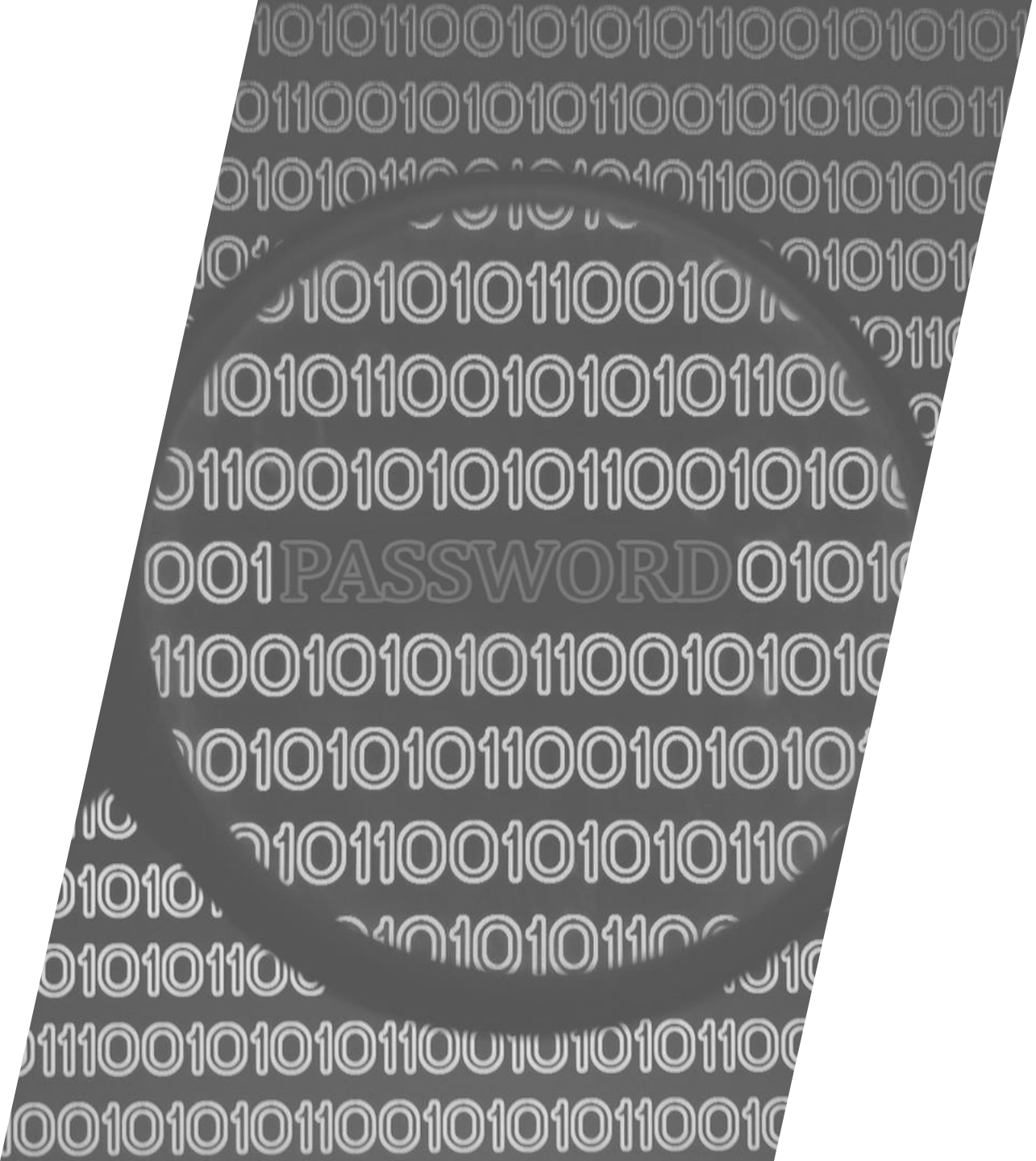
PASS HAX

PASSWORD GUESSER & EVALUATOR

TEAM YASH



CONTENTS

INTRODUCTION

OBJECTIVE

NEED FOR PROJECT

THREAT MODEL

APPLICATIONS

WORKING

VALUE GAINS

INTRODUCTION

WHAT'S THE IDEA?

- Passwords are important, efficient, easy to implement way of authorization & authentication.
- If used properly, they are very secure and cannot be cracked in short amount of time. Just an 18 character password with uppercase, lowercase letters, symbols numbers can take up to 438trillion years!
- PassHax creates a dictionary specific to a user as well as assists the user to empower their passwords and evaluate provided passwords

OBJECTIVE

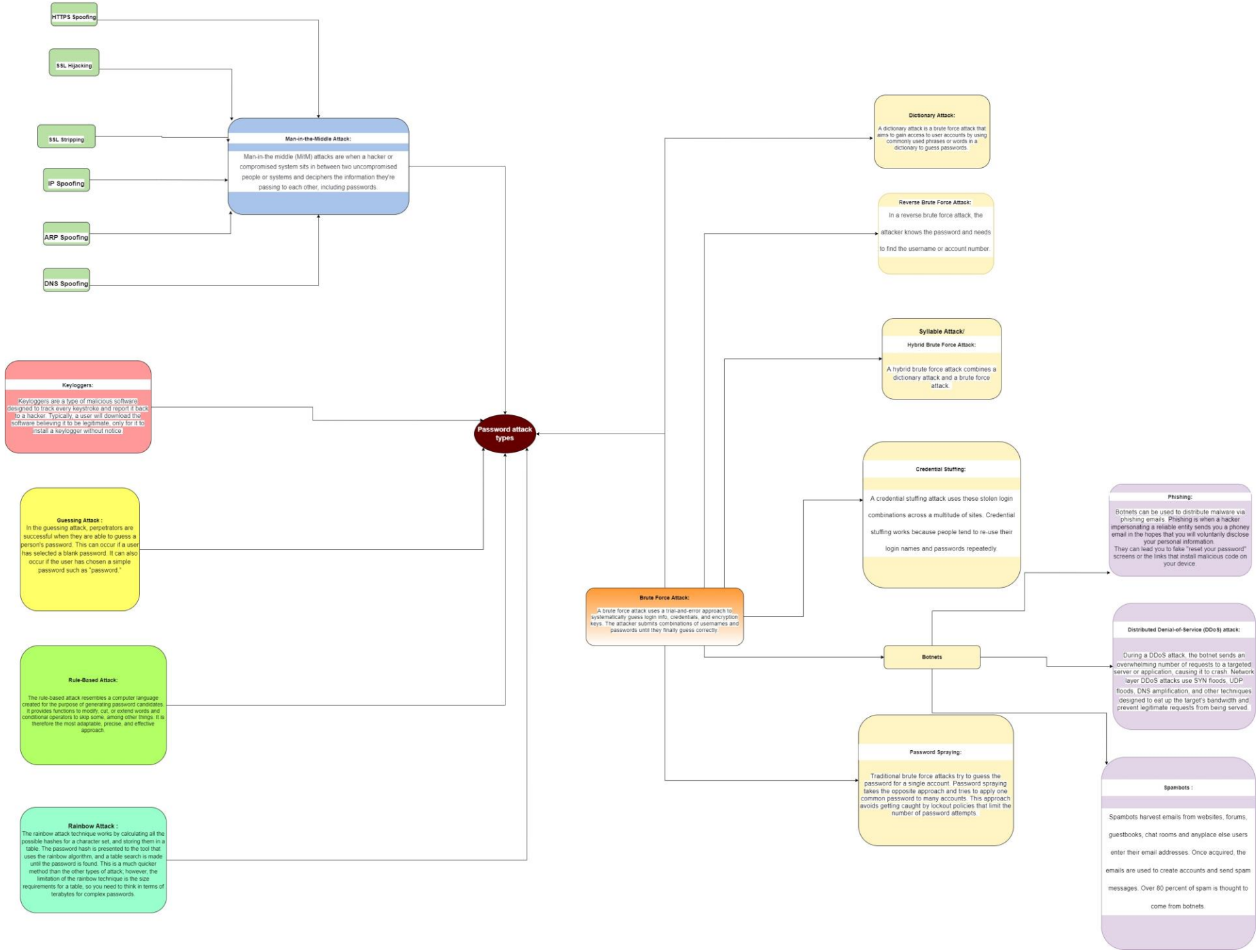
WHAT'S THE AIM?

- To help penetration testers to create user/target specific wordlists or dictionaries which can be used in brute force and dictionary exploits.
- To educate common users about how strong passwords are and can bridge the gap between being compromised by losing your data and staying secure.
- To guess passwords for an user & evaluate passwords provided by the user for their strength.

NEED FOR PASSHAX

WHY THIS TOOL?

- To eliminate common or obvious & repeating passwords.
- For better understanding of different password attacks. How common/obvious passwords can be easily exploited?
- Categorization of passwords such as weak, average or strong passwords.
- To know the time required to crack a particular password.
- Prevention mechanisms against different password attacks.
- To display the Strength and Score of passwords and then decide whether to use that particular password or not.


HTTPS Spoofing
SSL Hijacking
SSL Stripping
IP Spoofing
ARP Spoofing
DNS Spoofing
Man-in-the-Middle Attack:
Man-in-the middle (MitM) attacks are when a hacker or compromised system sits in between two uncompromised people or systems and deciphers the information they're passing to each other, including passwords.
Keyloggers:
Keyloggers are a type of malicious software designed to track every keystroke and report it back to a hacker. Typically, a user will download the software believing it to be legitimate, only for it to install a keylogger without notice.
Guessing Attack :
In the guessing attack, perpetrators are successful when they are able to guess a person's password. This can occur if a user has selected a blank password. It can also occur if the user has chosen a simple password such as "password."
Rule-Based Attack:
The rule-based attack resembles a computer language created for the purpose of generating password candidates. It provides functions to modify, cut, or extend words and conditional operators to skip some, among other things. It is therefore the most adaptable, precise, and effective approach.
Rainbow Attack :
The rainbow attack technique works by calculating all the possible hashes for a character set, and storing them in a table. The password hash is presented to the tool that uses the rainbow algorithm, and a table search is made until the password is found. This is a much quicker method than the other types of attack; however, the limitation of the rainbow technique is the size requirements for a table, so you need to think in terms of terabytes for complex passwords.
Password attack types
Dictionary Attack:
A dictionary attack is a brute force attack that aims to gain access to user accounts by using commonly used phrases or words in a dictionary to guess passwords.
Reverse Brute Force Attack:
In a reverse brute force attack, the attacker knows the password and needs to find the username or account number.
Syllable Attack/
Hybrid Brute Force Attack:
A hybrid brute force attack combines a dictionary attack and a brute force attack.
Credential Stuffing:
A credential stuffing attack uses these stolen login combinations across a multitude of sites. Credential stuffing works because people tend to re-use their login names and passwords repeatedly.
Brute Force Attack:
A brute force attack uses a trial-and-error approach to systematically guess login info, credentials, and encryption keys. The attacker submits combinations of usernames and passwords until they finally guess correctly.
Botnets
Phishing:
Botnets can be used to distribute malware via phishing emails. Phishing is when a hacker impersonating a reliable entity sends you a phoney email in the hopes that you will voluntarily disclose your personal information.
They can lead you to fake "reset your password" screens or the links that install malicious code on your device.
Distributed Denial-of-Service (DDoS) attack:
During a DDoS attack, the botnet sends an overwhelming number of requests to a targeted server or application, causing it to crash. Network layer DDoS attacks use SYN floods, UDP floods, DNS amplification, and other techniques designed to eat up the target's bandwidth and prevent legitimate requests from being served.
Password Spraying:
Traditional brute force attacks try to guess the password for a single account. Password spraying takes the opposite approach and tries to apply one common password to many accounts. This approach avoids getting caught by lockout policies that limit the number of password attempts.
Spambots :
Spambots harvest emails from websites, forums, guestbooks, chat rooms and anyplace else users enter their email addresses. Once acquired, the emails are used to create accounts and send spam messages. Over 80 percent of spam is thought to come from botnets.

APPLICATIONS

FOR WHOM?

- **PassHax** is a good tool for ethical hackers, penetration tester to generate personalized libraries for brute forcing as well as dictionary based attack.
- PassHax can guess passwords based on the answers you give to the ‘Security Questions’ and thus assist the user to create a stronger password.
- PassHax can be a first step towards the older age group to educate them more about cybersecurity and securing their assets with strong passwords.

VALUE GAIN

GIVERS GAIN

- **PassHax** will promote cybersecurity awareness amongst all citizens which will lead to a more safer & secured cyberspace, a safer cyberspace would surely be a gain for everyone.
- PassHax can be used for educational purposes to demonstrate how dictionary attacks work and how to prevent them.
- A large community using PassHax will increase the tool's reach further and would bring in more upgrades.

“ Treat your password like your toothbrush. Don't let anybody else use it, and get a new one every six months. ”

CLIFFORD STOLL

VISHWAKARMA UNIVERSITY
Maximising Human Potential

YASH

THANK YOU

YASH OSWAL
ATHARVA GOKHALE
SHIVANI SHETE
HASNAIN MERCHANT

TEAM YASH