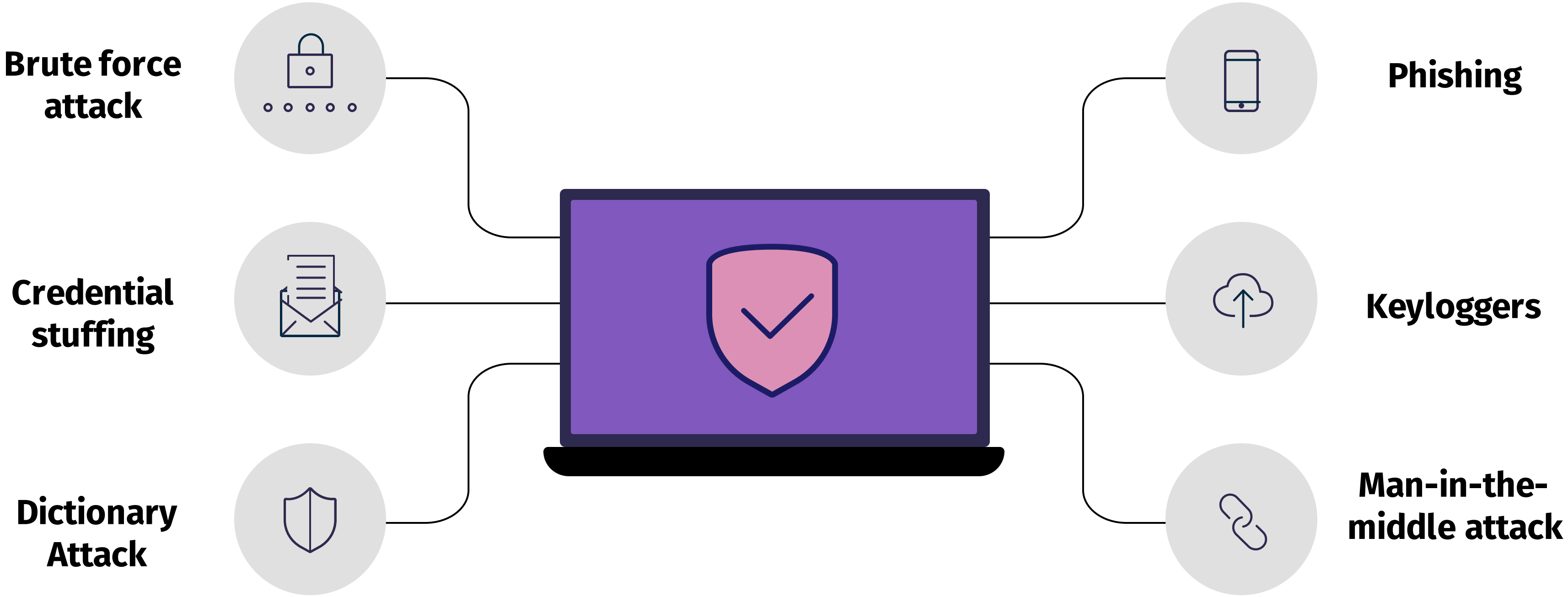
ETHICAL HACKING SERIES 1 PART 2

Social Engineering

- Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. In cybercrime, these “human hacking” scams tend to lure unsuspecting users into exposing data, spreading malware infections, or giving access to restricted systems. Attacks can happen online, in-person, and via other interactions.
- Scams based on social engineering are built around how people think and act. As such, social engineering attacks are especially useful for manipulating a user’s behavior. Once an attacker understands what motivates a user’s actions, they can deceive and manipulate the user.

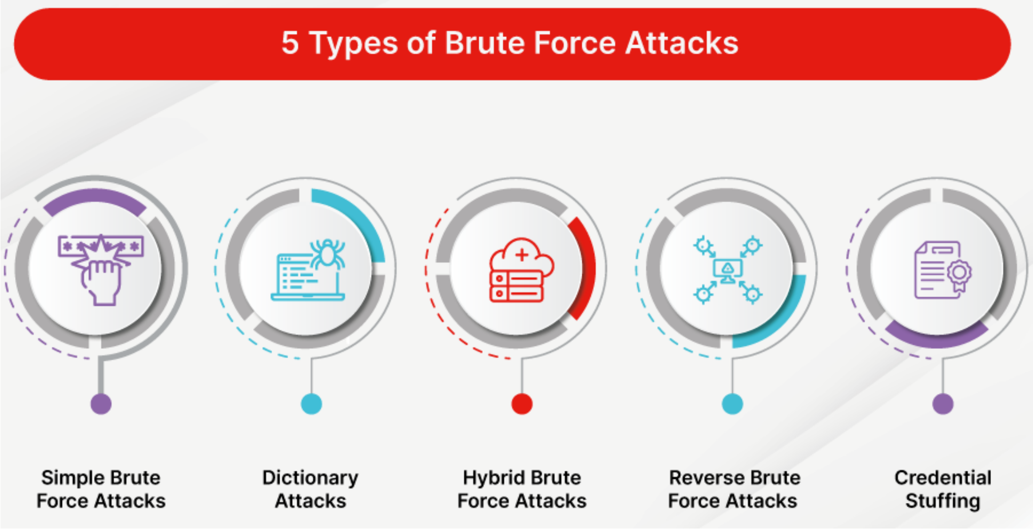
- Generally, social engineering attackers have one of two goals: Sabotage: Disrupting or corrupting data to cause harm or inconvenience. Theft: Obtaining valuables like information, access, or money.
- This process can take place in a single email or over months in a series of social media chats. It could even be a face-to-face interaction. But it ultimately concludes with an action you take, like sharing your information or exposing yourself to malware.
- Traits of Social Engineering Attacks Social engineering attacks center around the attacker's use of persuasion and confidence. When exposed to these tactics, you are more likely to take actions you otherwise wouldn't.
- There are some exceptions to these traits. In some cases, attackers use more simplistic methods of social engineering to gain network or computer access. For example, a hacker might frequent the public food court of a large office building and "shoulder surf" users working on their tablets or laptops.

Types of password attacks



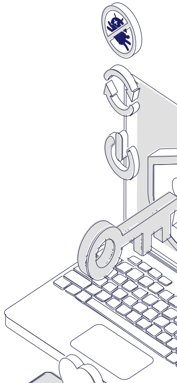
Brute force attack

A brute force attack is a hacking method that uses trial and error to crack passwords, login credentials, and encryption keys. It is a simple yet reliable tactic for gaining unauthorized access to individual accounts and organizations' systems and networks.



5 Types of Brute Force Attacks

- Simple Brute Force Attacks
- Dictionary Attacks
- Hybrid Brute Force Attacks
- Reverse Brute Force Attacks
- Credential Stuffing

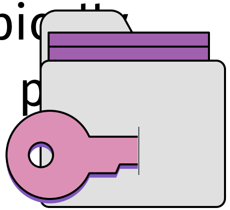


Credential stuffing

Credential stuffing is the automated injection of stolen username and password pairs (“credentials”) in to website login forms, in order to fraudulently gain access to user accounts.

Since many users will re-use the same password and username/email, when those credentials are exposed (by a database breach or phishing attack, for example) submitting those sets of stolen credentials into dozens or hundreds of other sites can allow an attacker to compromise those accounts too.

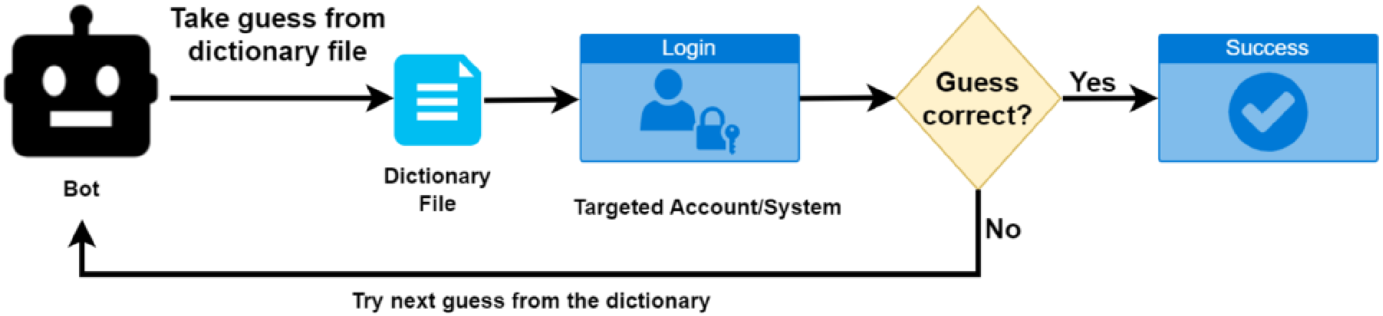
Credential Stuffing is a subset of the brute force attack category. Brute forcing will attempt to try multiple passwords against one or multiple accounts; guessing a password, in other words. Credential Stuffing typic refers to specifically using known (breached) username / password p against other websites.



Dictionary Attack

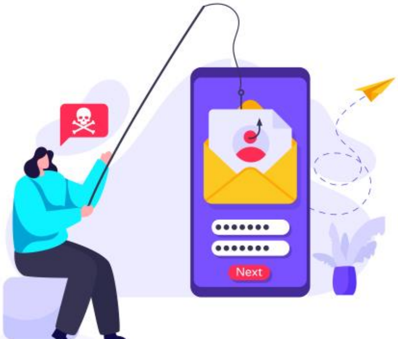
A dictionary attack is a type of brute force attack where hackers try to guess a user's password to their online accounts by quickly running through a list of commonly used words, phrases, and number combinations.

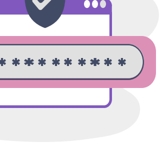
How Do Dictionary Attacks Work?



Phishing

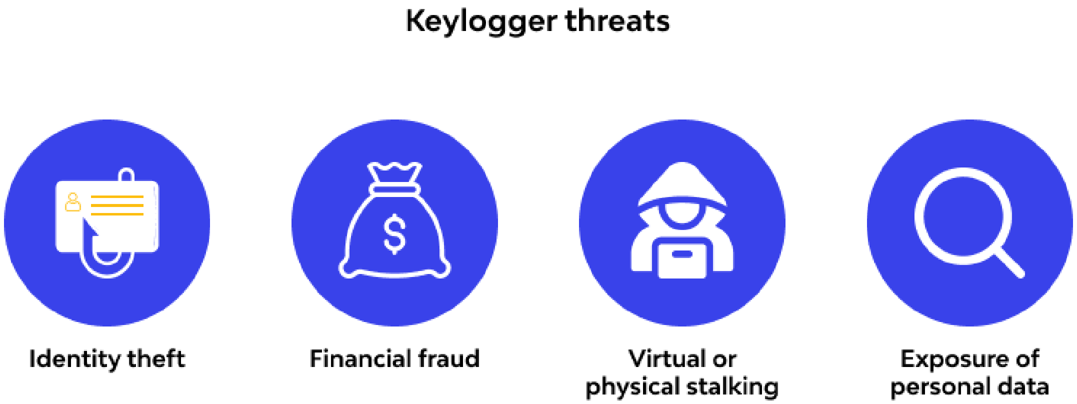
Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. It is usually done through email. The goal is to steal sensitive data like credit card and login information, or to install malware on the victim's machine.





Keyloggers

A keylogger, sometimes called a keystroke logger or keyboard capture, is a type of surveillance technology used to monitor and record each keystroke on a specific computer. Keylogger software is also available for use on smartphones, such as the Apple iPhone and Android devices.



Keylogger threats

Identity theft

Financial fraud

Virtual or physical stalking

Exposure of personal data

Man-in-the-middle attack

A man in the middle (MITM) attack is a general term for when a perpetrator positions himself in a conversation between a user and an application—either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is underway.The goal of an attack is to steal personal information, such as login credentials, account details and credit card numbers. Targets are typically the users of financial applications, SaaS businesses, e-commerce sites and other websites where logging in is required.

John The Ripper

John the Ripper is an Open Source password security auditing and password recovery tool available for many operating systems.

John The Ripper

John the Ripper jumbo supports hundreds of hash and cipher types, including: user passwords of Unix Flavors (Linux, *BSD, Solaris, AIX, QNX, etc.), macOS, Windows, "web apps" (e.g., WordPress), groupware (e.g., Notes/Domino), and database servers (SQL, LDAP, etc.); network traffic captures (Windows network authentication, Wi-Fi WPA-PSK, etc.); encrypted private keys (SSH, GnuPG, cryptocurrency wallets, etc.), filesystems and disks (macOS .dmg files and "sparse bundles", Windows BitLocker, etc.), archives (ZIP, RAR, 7z), and document files (PDF, Microsoft Office's, etc.) These are just some of the examples - there are many more.

Hashing Algorithms

- MD5: This is the fifth version of the Message Digest algorithm. MD5 creates 128-bit outputs. MD5 was a very commonly used hashing algorithm. That was until weaknesses in the algorithm started to surface. Most of these weaknesses manifested themselves as collisions. Because of this, MD5 began to be phased out.
- SHA-1: This is the second version of the Secure Hash Algorithm standard, SHA-0 being the first. SHA-1 creates 160-bit outputs. SHA-1 is one of the main algorithms that began to replace MD5, after vulnerabilities were found. SHA-1 gained widespread use and acceptance. SHA-1 was actually designated as a FIPS 140 compliant hashing algorithm.

- SHA-2: This is actually a suite of hashing algorithms. The suite contains SHA-224, SHA-256, SHA-384, and SHA-512. Each algorithm is represented by the length of its output. SHA-2 algorithms are more secure than SHA-1 algorithms, but SHA-2 has not gained widespread use.
- LANMAN: Microsoft LANMAN is the Microsoft LAN Manager hashing algorithm. LANMAN was used by legacy Windows systems to store passwords. LANMAN used DES algorithms to create the hash. The problem is that LANMAN's implementation of the DES algorithm isn't very secure, and therefore, LANMAN is susceptible to brute force attacks. LANMAN password hashes can actually be cracked in just a few hours. Microsoft no longer uses LANMAN as the default storage mechanism. It is available, but is no longer turned on by default.
- NTLM: This is the NT LAN Manager algorithm. The NTLM algorithm is used for password hashing during authentication. It is the successor of the LANMAN algorithm. NTLM was followed with NTLMv2. NTLMv2 uses an HMAC-MD5 algorithm for hashing.

Cracking Modes in JtR

01

Single Crack Mode

john [file]: This command starts the password cracking process on the specified file.

02

Incremental Mode

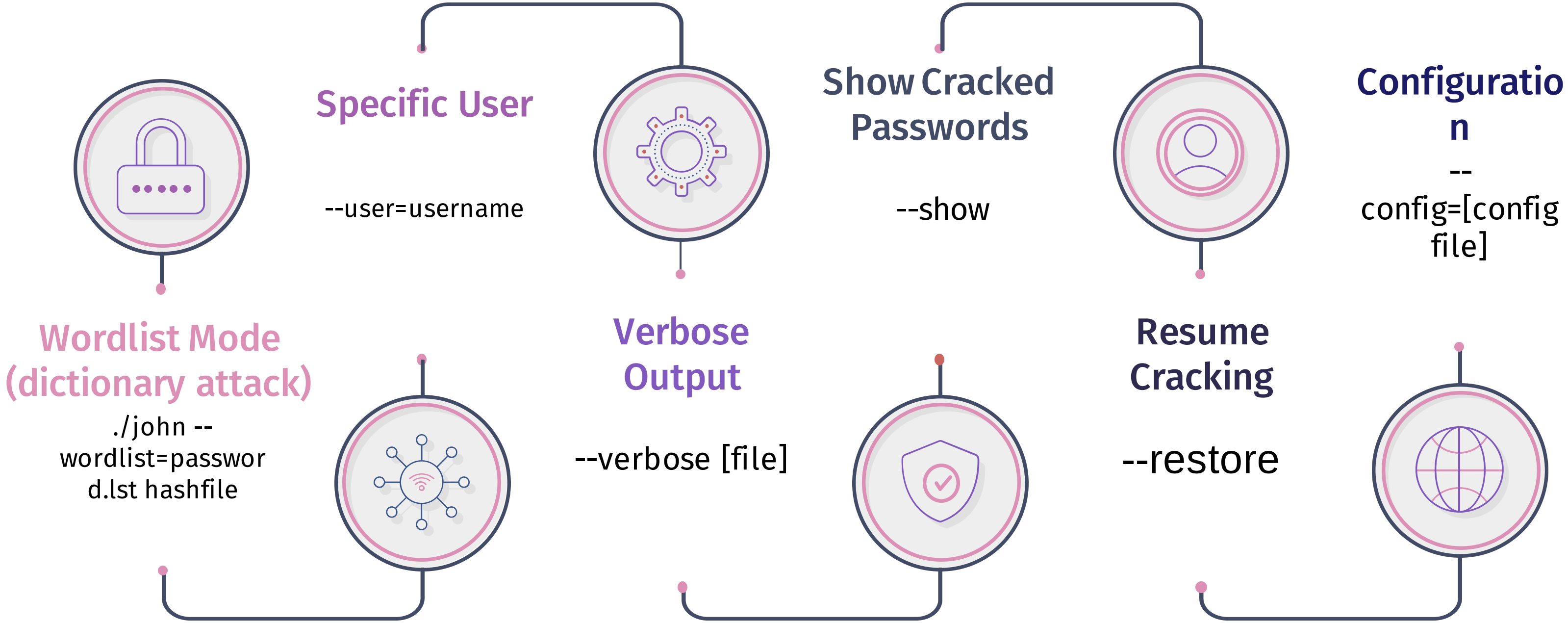
john --incremental [file]: This command tells John to use incremental mode, where it tries all possible password combinations.

03

Wordlist Mode

john --wordlist/-w =[wordlist file] [file]: This command tells John to use a specific wordlist for password cracking.

Commonly used modifiers



Wordlist Mode (dictionary attack)

`./john --wordlist=password.lst hashfile`

Specific User

`--user=username`

Verbose Output

`--verbose [file]`

Show Cracked Passwords

`--show`

Resume Cracking

`--restore`

Configuration

`--config=[config file]`

THANKS!

Presentation by:

Abhishek
Achintya Chaitanya
Manan Singh