Chapter 5. 2FA and Brute Force attacking

Chapter 5.Sections and sectors

1. 2FA authentification

1.1What is 2FA authentification?

1.2 What are the types of 2FA?

1.3 What are the Factors of Authentication

2. Bruce force attacking

2.1 What is Brute force attacking?

2.2 Types of Brute Force Attacks

2.3 Brute Force Attack Tools. How to prevent brute force attacks?

1.1 Two-factor authentication (2FA)

- Two-factor authentication (2FA) is a specific type of multi-factor authentication (MFA) that strengthens access security by requiring two methods (also referred to as authentication factors) to verify your identity.
- These factors can include something you know — like a username and password — plus something you have — like a smartphone app — to approve authentication requests.
- 2FA protects against phishing, social engineering and password brute-force attacks and secures your logins from attackers exploiting weak or stolen credentials.

Why is 2FA Important?

- Two-factor authentication (2FA) is the foundational element of a zero trust security model. In order to protect sensitive data, you must verify that the users trying to access that data are who they say they are. 2FA is an effective way to protect against many security threats that target user passwords and accounts, such as phishing, brute-force attacks, credential exploitation and more.
- By integrating two-factor authentication with your applications, attackers are unable to access your accounts without possessing your physical device needed to complete the second factor.

What are the types of 2FA?

- There are a number of different second factors that can be used to verify a user's identity. From passcodes to biometrics, the available options address a range of use cases and protection levels.

What are the types of 2FA?

SMS 2FA

- Simplicity.
- Speed and access.
- Ubiquitousness.
- Phone number requirements
- Data network requirements.

What are the types of 2FA?
TOTP 2FA

- The Time-Based One Time Password (TOTP) 2FA method generates a key locally on the device a user is attempting to access.

Flexibility

Reliance on devices.

Improved Access.

What are the types of 2FA?
Push-Based 2FA

- Push-based 2FA improves on SMS and TOTP 2FA by adding additional layers of security, while improving ease of use for end users.

Phishing security.

Ease of use.

Scalable.

Reliance on data access.

Reliance on user knowledge.

What are the types of 2FA?
WebAuthn

Created by the FIDO (Fast IDentity Online) Alliance and W3C, the Web Authentication API is a specification that enables strong, public key cryptography registration and authentication.

Convenience.

More secure.

Scalable.

Complex account recovery.

Reliance on user knowledge.

Which industries use 2FA?

Government

Energy

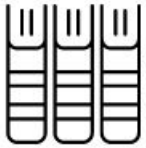
Healthcare

Travel

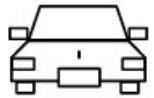
Media

Retail

Social Media



Higher Education



Ridesharing

What are the Factors of Authentication?

- Knowledge Factor
- Inherence Factor
- Time Factor
- Possession Factor
- Location Factor

What Threats Does 2FA Address?

- Stolen Passwords
- Social Engineering
- Key Logging
- Phishing Attempts
- Brute-Force Attacks

2FA To The Rescue

- 2FA is an extra layer of security used to make sure that people trying to gain access to an online account are who they say they are. First, a user will enter their username and a password. Then, instead of immediately gaining access, they will be required to provide another piece of information. This second factor could come from one of the following categories:

- **Something you know:** This could be a personal identification number (PIN), a password, answers to "secret questions" or a specific keystroke pattern
- **Something you have:** Typically, a user would have something in their possession, like a credit card, a smartphone, or a small hardware token
- **Something you are:** This category is a little more advanced, and might include biometric pattern of a fingerprint, an iris scan, or a voice print

Common Types of 2FA
Hardware Tokens for 2FA

- Probably the oldest form of 2FA, hardware tokens are small, like a key fob, and produce a new numeric code every 30-seconds. When a user tries to access an account, they glance at the device and enter the displayed 2FA code back into the site or app. Other versions of hardware tokens automatically transfer the 2FA code when plugged into a computer's USB port.

Common Types of 2FA
SMS Text-Message and Voice-based 2FA

- SMS-based 2FA interacts directly with a user's phone. After receiving a username and password, the site sends the user a unique one-time passcode (OTP) via text message. Like the hardware token process, a user must then enter the OTP back into the application before getting access. Similarly, voice-based 2FA automatically dials a user and verbally delivers the 2FA code. While not common, it's still used in countries where smartphones are expensive, or where cell service is poor.

Common Types of 2FA
SMS Text-Message and Voice-based 2FA

- The most popular form of two-factor authentication (and a preferred alternative to SMS and voice) uses a software-generated time-based, one-time passcode (also called TOTP, or “soft-token”).
- First, a user must download and install a free 2FA app on their smartphone or desktop. They can then use the app with any site that supports this type of authentication. At sign-in, the user first enters a username and password, and then, when prompted, they enter the code shown on the app. Like hardware tokens, the soft-token is typically valid for less than a minute. And because the code is generated and displayed on the same device, soft-tokens remove the chance of hacker interception. That’s a big concern with SMS or voice delivery methods.

Common Types of 2FA
Push Notification for 2FA

- Rather than relying on the receipt and entry of a 2FA token, websites and apps can now send the user a push notification that an authentication attempt is taking place. The device owner simply views the details and can approve or deny access with a single touch. It's passwordless authentication with no codes to enter, and no additional interaction required.

- https://www.youtube.com/watch?v=ds_TANz4n3U&t=1s&ab_channel=Authy

2. Brute Force Attack Definition

- 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.

Types of Brute Force Attacks
1. Simple Brute Force Attacks

- A simple brute force attack occurs when a hacker attempts to guess a user's login credentials manually without using any software. This is typically through standard password combinations or personal identification number (PIN) codes.

Types of Brute Force Attacks
2. Dictionary Attacks

- A dictionary attack is a basic form of brute force hacking in which the attacker selects a target, then tests possible passwords against that individual's username. The attack method itself is not technically considered a brute force attack, but it can play an important role in a bad actor's password-cracking process.

Types of Brute Force Attacks
3. Hybrid Brute Force Attacks

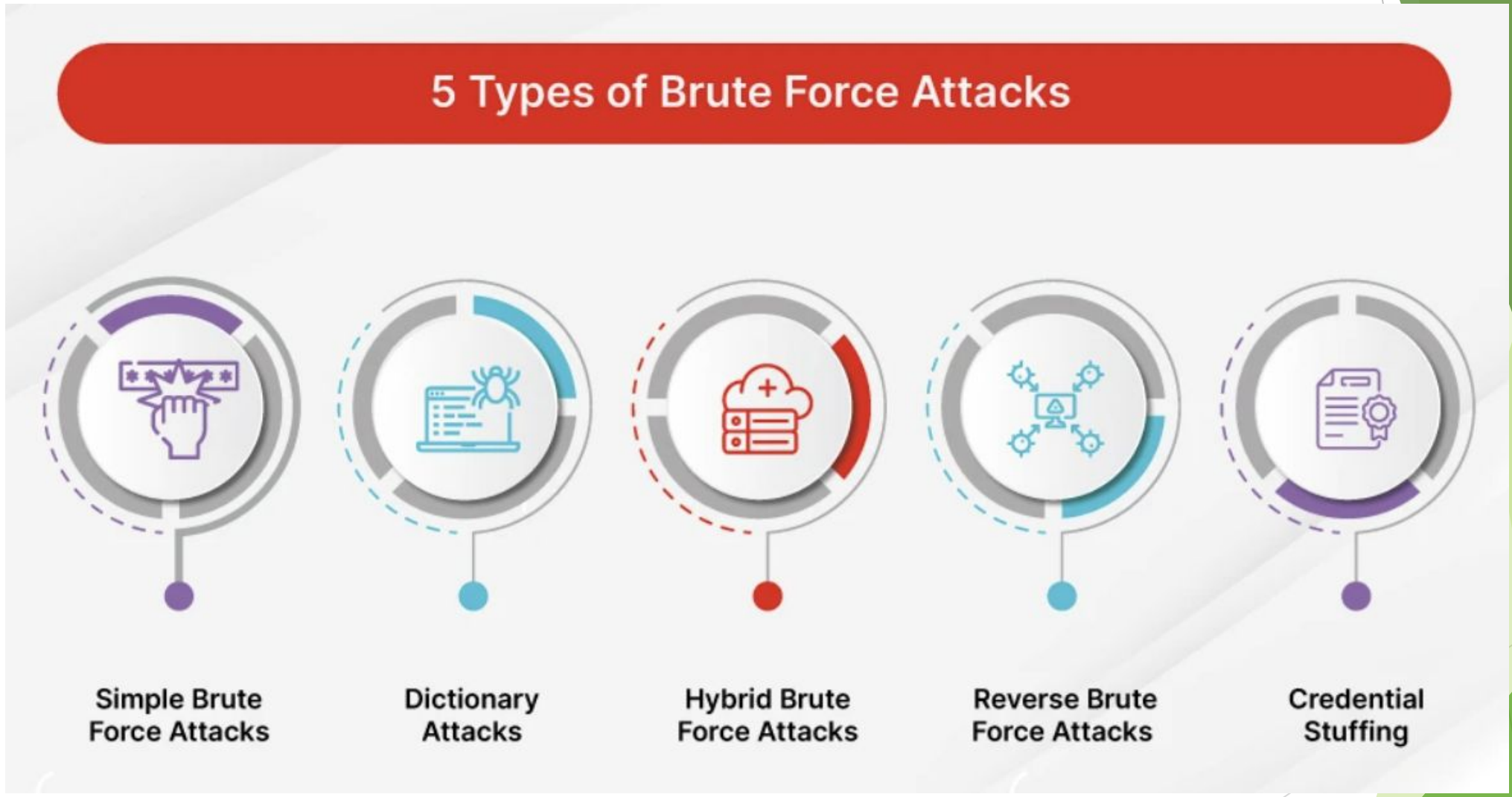
- A hybrid brute force attack is when a hacker combines a dictionary attack method with a simple brute force attack. It begins with the hacker knowing a username, then carrying out a dictionary attack and simple brute force methods to discover an account login combination.

Types of Brute Force Attacks
4. Reverse Brute Force Attacks

- A reverse brute force attack sees an attacker begin the process with a known password, which is typically discovered through a network breach. They use that password to search for a matching login credential using lists of millions of usernames. Attackers may also use a commonly used weak password, such as "Password123," to search through a database of usernames for a match.

Types of Brute Force Attacks
5. Credential Stuffing

- Credential stuffing preys on users' weak password etiquettes. Attackers collect username and password combinations they have stolen, which they then test on other websites to see if they can gain access to additional user accounts. This approach is successful if people use the same username and password combination or reuse passwords for various accounts and social media profiles.


5 Types of Brute Force Attacks
Simple Brute Force Attacks
Dictionary Attacks
Hybrid Brute Force Attacks
Reverse Brute Force Attacks
Credential Stuffing

What is the Motive Behind Brute Force Attacks?

- Exploit Ads or Activity Data
- Steal Personal Data
- Spread Malware
- Hijack Systems for Malicious Activity
- Ruin a Company or Website's Reputation

What is the Motive Behind Brute Force Attacks?

Exploit Ads or Activity Data

- A hacker may launch a brute force attack on a website or multiple websites to earn financial profit from advertising commission. Common methods include:

1. Placing spam ads on popular websites, which enables the attacker to earn money every time an ad gets clicked or viewed by a visitor.
2. Rerouting traffic to a legitimate website to illegal commissioned ad sites.
3. Infecting a website and site visitors with malware, such as spyware, that tracks activity. The data collected is then sold to advertisers without the user's consent.

What is the Motive Behind Brute Force Attacks?

Steal Personal Data

- Hacking into a user's personal accounts can provide a treasure trove of data, from financial details and bank accounts to confidential medical information. Access to an account enables an attacker to spoof a person's identity, steal their money, sell their credentials to third parties, or use the information to launch wider attacks.
- Personal data and login credentials can also be stolen through corporate data breaches that see attackers gain access to organizations' sensitive databases.

What is the Motive Behind Brute Force Attacks?

Spread Malware

- Brute force attacks are often not personal. A hacker may simply want to create havoc and showcase their malicious skills. They may do this by spreading malware via email or Short Message Service (SMS) messages, concealing malware within a spoofed website designed to look like a legitimate site, or redirecting website visitors to malicious sites.
- By infecting a user's computer with malware, the attacker can then work their way into connected systems and networks and launch wider cyberattacks against organizations.

What is the Motive Behind Brute Force Attacks?

Hijack Systems for Malicious Activity

- Brute force attacks can play a role in malicious actors launching broader attacks using multiple devices, called a botnet. This is typically a distributed denial-of-service (DDoS) attack that aims to overpower the target's security defenses and systems.

What is the Motive Behind Brute Force Attacks?

Ruin a Company or Website's Reputation

- Brute force attacks are often launched in an attempt to steal data from an organization, which not only costs them financially but also causes huge reputational damage. Websites can also be targeted with attacks that infest them with obscene or offensive text and images, thereby denigrating their reputation, which could lead to them being taken down.

Brute Force Attack Tools

- Brute force attack tools include password-cracking applications, which crack username and password combinations that would be extremely difficult for a person to crack on their own. Commonly used brute force attack tools include:

Aircrack-ng

John the Ripper

How to Prevent Brute Force Attacks

Use Stronger Password Practices

Better Protect User Passwords

Provide Ongoing Security and Password Support

What is an Encryption Key?

- Encryption is a cybersecurity tactic that scrambles data so it appears as a string of random characters. The correct encryption key will unscramble the data.
- A 128-bit encryption key would require two to the power of 128 combinations to crack, which is impossible for most powerful computers. Most websites and web browsers use it. 256-bit encryption makes data protection even stronger, to the point that even a powerful computer that can check trillions of combinations every second would never crack it. This makes 256-bit encryption completely immune to brute force attacks.