This Password Manager, stores your passwords disconnected and off the internet such as on a removable memory card*

Online

Offline

This is simply a collection of compromised computers or Internet of Things (IoT) devices under the control of a master node. This is a part of command and control node controls not just your computer, but hundreds or thousands or hundreds of thousands of other computers.*

Virus

Ransomware

Worm

Botnet

This is a piece of text stored on a user's computer by their web browser which is place on your computer after your initial login.*

URL

SMTP

Cookie

SSL

HTTP

This is a secret string of 8 to 10 characters that must be used to gain admission to something like a computer system or web service.*

Password

Decrypt

Encrypt

Passphrase

In this type of password attack, stolen user accounts names and passwords are going to be tested against multiple websites in an effort to bypass their authentication. This is used by attackers and penetration testers because many users often will use the same usernames and passwords on many different websites.*

Credential Stuffing

Password Spraying

Dictionary Attack

Bruteforce Attack

This is a Security Aspects of Online Banking that integrated fingerprint, facial identification, and voice recognition authentication into their mobile banking apps.*

Limited Liability

Biometric Authentication

Automatic Logout

Secure Socket Layer

This is a system of communication where only the people communicating with each other can read the message they send. Nobody can access the cryptographic keys needed to convert the conversation into readable plaintext*

End-To-End Encryption

One Time PIN

VPN

Two Way Authentication

This Password Managers typically store your passwords and other information in the cloud or on your device, both of which are connected to the internet*

Online

Offline

This is a Security Aspects of Online Banking that depending on the terms of the policy, your liability for unauthorized transactions is limited. In other words, if you report unauthorized transactions on your account in a timely manner, the charges may not be your responsibility.*

Security Socket Layer

Biometric Authentication

Automatic Logout

Limited Liability

The attacker creates a large number of processes to use up available processing power of a computer. This spread out inside the processor's cache on a single computer that it's being attacked with, and it causes a denial-of-service attack and a denial-of-service condition.*

Fork Bomb

Ping Flood

Permanent Denial-of-Service attack (PDoS)

Flood Attack

This is an Access Security Framework that makes sure that the tracking of data, computer usage, and network resources is maintained.*

Password

Authentication

Authorization

Accounting

This is used to create and extend a private network across a public network so the traffic is not observable by someone outside of the tunnel.*

Intrusion Detection and Prevention System

Firewall

Antivirus

Virtual Private Network (VPN)

This is a Security Aspects of Online Banking that automatically log you out of your secure session after a period of inactivity to help prevent others from seeing or using your online accounts.*

Secure Socket Layer

Limited Liability

Automatic Logout

Biometric Authentication

This is a long string of three or four words that must be used to gain access to a computer system or web service.*

Password

Passphrase

Encrypt

Decrypt

This attack uses a list of common passwords to attempt to guess the password. This password guessing tool then hashes the value of the individual dictionary listing and compares it to the hash value of the password inside of the system file.*

Rainbow Table

Password Spraying

Bruteforce Attack

Dictionary Attack

This technique in surviving DDoS attacks identifies attacking IP addresses and routes all of their traffic to a non-existent server through a null interface. This technique identifies attacking IP addresses and routes all of their traffic to a non-existent server through a null interface.*

Blockholing or Sinkholing

Fork Bomb

Flood Attack

Ping Flood

The easiest way to access the Darknet is through the ___________________, which lets you surf both the clear and dark web.*

Safari

Tor Browser

Google Chrome

Microsoft Edge

In this VPN make your online activity anonymous and can make you appear to be accessing the internet in a different physical location. This avoids surveillance, accessing websites your government, school, or workplace blocks, or your ISP monitors, as well as watching streaming content that's only available in certain countries*

Firewall

Site-to-Site VPN

Client-to-Site VPN

Commercial VPN

This is the heart of most authentication systems.*

Username

Security

Email Address

Password

This attack is a great option if you're trying to crack a pin or password with a very limited key space, for example Wi-Fi protected setup (WPS) PINs are eight digit numbers but they're actually composed of two, four digit numbers.*

Dictionary Attack

Password Spraying

Rainbow Table

Bruteforce Attack

This is a form of password guessing that focuses on using the same few commonly used passwords across multiple accounts in an attempt to bypass the authentication mechanisms.*

Dictionary Attack

Password Spraying

Bruteforce Attack

Rainbow Table

This protocol creates a secure connection with your browser when you log in, fill out an application, register for services and more. To secure online banking this type of encryption is used.*

Hypertext Transfer Protocol (HTTP)

Secure Socket Layer (SSL)

Uniform Resource Locator (URL)

Simple Mail Transfer Protocol (SMTP)

In this VPN, we can connect a single person's device to private corporate network over the public Internet. We're going to be sending data from a single device, like a laptop or cell phone and connecting it back to our headquarters office. This is going to be done instead of going from router to router, we're going from client to router. This allows a remote user to be able to connect back to the headquarters.*

Client-to-Site VPN

Site-to-Site VPN

Commercial VPN

Intrusion Detection and Prevention System

Password Manager will create a unique, strong password for every website you visit and you only have to remember a single passphrase to access them all. You can have hundreds or thousands of different passwords and you can control them all from within the password manager and you only have to memorize one passphrase.*

False

True

This is an Access Security Framework that occurs when a person's identity is established with proof and is confirmed by the system*

Password

Authorization

Authentication

Accounting

This is an authentication technology that enables a person to authenticate once, and then receive the ability to access multiple services without authenticating to each one separately. When you use single sign on, you don't have to use multiple usernames and passwords. Instead, you should have one nice, strong password that you can memorize and then use to get on to everything, because you log on once and have access to all the systems.*

Username

Email Address

Single Sign On (SSO)

Password

This is an Access Security Framework that occurs when a user is given to a certain piece of data or certain areas of a building.*

Authorization

Authentication

Password

Accounting

Instead of using a single attack targeting one server, they use hundreds or even thousands of machines to launch an attack simultaneously against a single server and force it offline to create that denial-of-service condition. Generally, these machines have become zombies or bots inside a large botnet, and then when they receive that command to attack, they all simultaneously send all of their payloads against a single victim.*

Distributed Denial-of-Service (DDoS)

Denial-of-Service

Password Attack

Brute Force Attack

In this VPN we can connect two offices together over the public Internet. This VPN gateway from one Local Area Network communicates with the VPN Gateway of another LAN and creates a secure VPN Tunnel*

Intrustion Detection and Prevention System

Site-to-Site VPN

Commercial VPN

Client-to-Site VPN

This is an attack which exploits a security flaw to permanently break a networking device by reflashing its firmware.*

Permanent Denial-of-Service attack (PDoS)

Flood Attack

Ping Flood

Fork Bomb

This attack attempt to break a password by guessing every single possible combinations of numbers, letters, or special characters.*

Bruteforce Attack

Password Spraying

Rainbow Table

Dictionary Attack

This includes strong cryptography and key management. This is an agreement that any organization that collects, stores or processes credit card customers information has to abide by. This is not actually a law or regulation but instead, it's a contractual agreement and standard that must be followed if the organization wants to handle credit card transactions.*

Payment Card Industry Data Security Standard (PCI-DSS)

Biometric Authentication

Secure Socket Layer

Automatic Logour