



MAY - 26 - 24

A — Z *Of* CYBERSECURITY

FOLLOW @ ONYEDIKA SOMTO
#CybersecurityBible
#OnyedikaSomto



MAY - 26 - 24

A Antivirus

A Software designed to detect, prevent, and remove malware by scanning and identifying threats.

FOLLOW @ ONYEDIKA SOMTO
#CybersecurityBible
#OnyedikaSomto



MAY - 26 - 24

B Backdoor

A secret entrance to a system that bypasses normal security measures, allowing unauthorized access.

FOLLOW @ ONYEDIKA SOMTO
#CybersecurityBible
#OnyedikaSomto



MAY - 26 - 24

Cryptography.

The practice of securing information by transforming it into unreadable formats, ensuring confidentiality and integrity.

FOLLOW @ ONYEDIKA SOMTO
#CybersecurityBible
#OnyedikaSomto



MAY - 26 - 24

D

DDoS (Distributed Denial of Service)

An attack that aims to make a service unavailable by overwhelming it with traffic from multiple sources.

FOLLOW @ ONYEDIKA SOMTO
#CybersecurityBible
#OnyedikaSomto



MAY - 26 - 24

E

Encryption

The process of converting plaintext into ciphertext to protect data from unauthorized access.

FOLLOW @ ONYEDIKA SOMTO
#CybersecurityBible
#OnyedikaSomto



MAY - 26 - 24

F

Firewall

A network security device or software that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

[FOLLOW](#) @ ONYEDIKA SOMTO
[#CybersecurityBible](#)
[#OnyedikaSomto](#)



MAY - 26 - 24

G

Gateway

A network point that acts as an entrance to another network, often used for securing and managing traffic.

FOLLOW @ ONYEDIKA SOMTO
#CybersecurityBible
#OnyedikaSomto



MAY - 26 - 24

H

Hashing

Hashing converts data into a fixed-length hash value for various functions, including data integrity, password storage, and message authentication.

FOLLOW @ ONYEDIKA SOMTO
#CybersecurityBible
#OnyedikaSomto



MAY - 26 - 24

IDS (Intrusion Detection System).

A system that monitors network or system activities for malicious actions or policy violations.

FOLLOW @ ONYEDIKA SOMTO
#CybersecurityBible
#OnyedikaSomto



MAY - 26 - 24

J

Jailbreaking

The process of removing restrictions on devices, which may potentially lead to vulnerabilities.

FOLLOW @ ONYEDIKA SOMTO
#CybersecurityBible
#OnyedikaSomto



MAY - 26 - 24

K

Keylogger

Malware that records keystrokes to steal sensitive information such as passwords and credit card numbers.

FOLLOW @ ONYEDIKA SOMTO
#CybersecurityBible
#OnyedikaSomto



MAY - 26 - 24



Log Analysis

The process of reviewing and interpreting log data to detect and investigate security incidents.

FOLLOW @ ONYEDIKA SOMTO
#CybersecurityBible
#OnyedikaSomto



MAY - 26 - 24

M Malware

A Malicious software designed to harm,
exploit, or compromise the data and
systems of a target.

FOLLOW @ ONYEDIKA SOMTO
#CybersecurityBible
#OnyedikaSomto



MAY - 26 - 24

N Nmap

A network scanning tool used to discover devices and services on a computer network.

FOLLOW @ ONYEDIKA SOMTO
#CybersecurityBible
#OnyedikaSomto



MAY - 26 - 24

Operating System

The software that supports a computer's basic functions, like Windows, macOS, or Linux.

FOLLOW @ ONYEDIKA SOMTO
#CybersecurityBible
#OnyedikaSomto



MAY - 26 - 24

p

Phishing

A fraudulent attempt to obtain sensitive information by pretending to be a trustworthy entity via email or other channels.

FOLLOW @ ONYEDIKA SOMTO
#CybersecurityBible
#OnyedikaSomto



MAY - 26 - 24



Quishing

A type of phishing attack that uses QR codes (Quick Response codes) to trick victims into revealing sensitive information or downloading malware.

FOLLOW @ ONYEDIKA SOMTO
#CybersecurityBible
#OnyedikaSomto



MAY - 26 - 24

R Ransomware

A type of malware that encrypts a victim's files, demanding payment to restore access.

FOLLOW @ ONYEDIKA SOMTO
#CybersecurityBible
#OnyedikaSomto



MAY - 26 - 24

S

SSL (Secure Sockets Layer)

A standard security technology for establishing an encrypted link between a server and a client, usually a web server and a browser.

FOLLOW @ ONYEDIKA SOMTO
#CybersecurityBible
#OnyedikaSomto



MAY - 26 - 24

T

Two-Factor Authentication (2FA)

An additional layer of security requiring not only a password and username but something that only the user has on them, such as a physical token or a mobile phone.

FOLLOW @ ONYEDIKA SOMTO
#CybersecurityBible
#OnyedikaSomto



MAY - 26 - 24

U

UDP (User Datagram Protocol)

A communication protocol used for time-sensitive transmissions like online gaming, video streaming where speed is more important than accuracy.

FOLLOW @ ONYEDIKA SOMTO
#CybersecurityBible
#OnyedikaSomto



MAY - 26 - 24

VPN (Virtual Private Network).

A service that encrypts internet connections
to secure the transfer of data and maintain
user privacy online.

FOLLOW @ ONYEDIKA SOMTO
#CybersecurityBible
#OnyedikaSomto



MAY - 26 - 24

W Worm

A type of malware that replicates itself to spread to other computers, often exploiting network vulnerabilities.

FOLLOW @ ONYEDIKA SOMTO
#CybersecurityBible
#OnyedikaSomto



MAY - 26 - 24



XSS (Cross-Site Scripting)

The process of Injecting malicious scripts into trusted websites.

FOLLOW @ ONYEDIKA SOMTO
#CybersecurityBible
#OnyedikaSomto



MAY - 26 - 24

Y

Yubikey.

A hardware authentication device that supports one-time passwords, public key encryption, and authentication.

FOLLOW @ ONYEDIKA SOMTO
#CybersecurityBible
#OnyedikaSomto



MAY - 26 - 24

Z

Zombie system

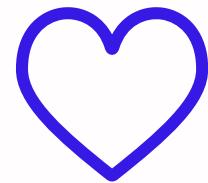
A computer that has been compromised by a hacker and is being used to perform malicious tasks without the owner's knowledge.

FOLLOW @ ONYEDIKA SOMTO
#CybersecurityBible
#OnyedikaSomto

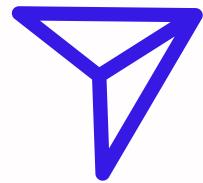


MAY - 26 - 24

Do you find this helpful?



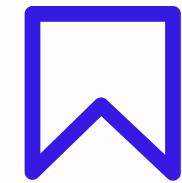
LIKE



SHARE



COMMENT



SAVE

[Follow @OnyedikaSomto](#)

[FOLLOW @ ONYEDIKA SOMTO](#)
[#CybersecurityBible](#)
[#OnyedikaSomto](#)