Cheat Sheets

Cybersecurity Acronyms

CYBERSECURITY ACRONYMS (PART 1)

@SECURITYTRYBEE

*CIA - CONFIDENTIALITY, INTEGRITY, AVAILABILITY

*IDS - INTRUSION DETECTION SYSTEM

*IPS - INTRUSION PREVENTION SYSTEM

*WAF - WEB APPLICATION FIREWALL

*PII - PERSONAL IDENTIFIABLE INFORMATION

*DOS - DENIAL OF SERVICE

*DDOS - DISTRIBUTED DENIAL OF SERVICE

*DNS - DOMAIN NAME SYSTEM

*ZTA - ZERO TRUST ARCHITECTURE

*NAT - NETWORK ADDRESS TRANSLATION

*CTF - CAPTURE THE FLAG

*ACL - ACCESS CONTROL LIST

*CDN - CONTENT DELIVERY NETWORK

*CVE - COMMON VULNERABILITIES AND EXPOSURES

Common types of password attacks

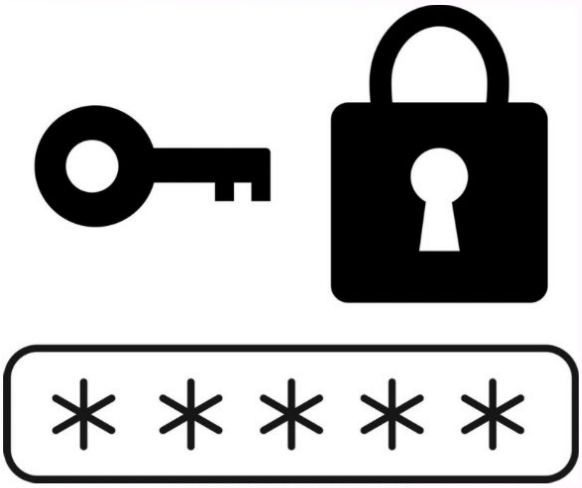
SECURITY TRYBE

COMMON TYPES OF PASSWORD ATTACKS

Brute Force Attack:
Hackers use software to guess various password combinations until they crack the code.

Keylogger:
Malicious software records keystrokes, capturing passwords as users type.

Social Engineering:
Hackers create fake websites resembling legitimate login pages. When users enter their information, it gets recorded.

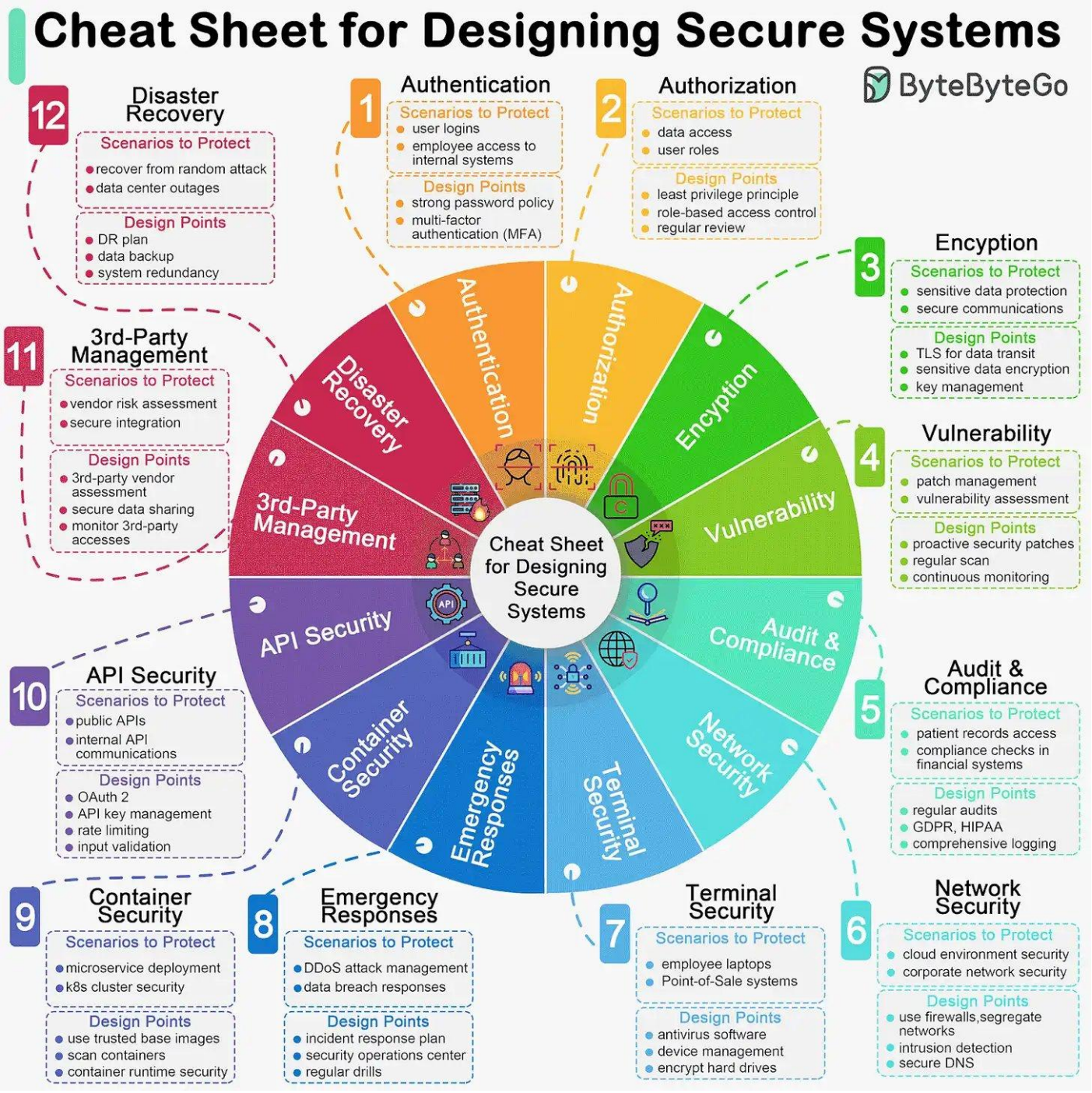


Rainbow Table Attack:
This type of password crack uses pre-computed table of all possible hashes of all possible passwords

Credential Stuffing:
Cybercriminals exploit stolen credentials (such as usernames and passwords) to break into accounts.

Dictionary Attack:
Similar to brute force attacks, dictionary attacks rely on common phrases or dictionary words as passwords.

Designing Secure Systems



Revision #5
Created 17 October 2024 19:49:30 by Admin
Updated 5 December 2024 19:51:53 by Admin