

# 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

# COMMON TYPES OF PASSWORD ATTACKS



## Brute Force Attack:

Hackers use software to guess various password combinations until they crack the code.



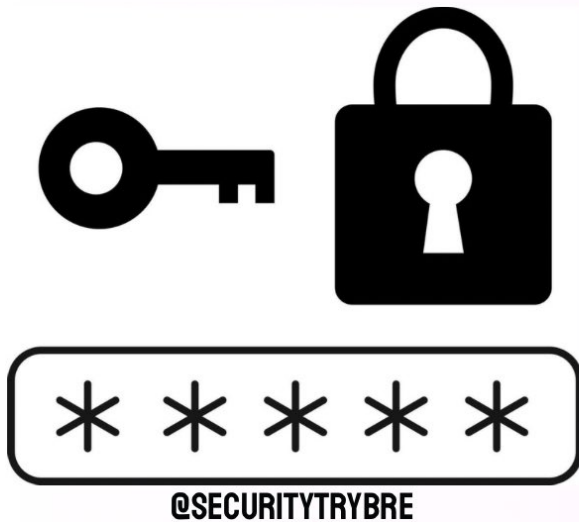
## Keylogger:

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.



@SECURITYTRYBE

## Rainbow Table Attack:

This type of password crack uses pre-computed table of all possible hashes of all possible passwords



## Dictionary Attack:

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

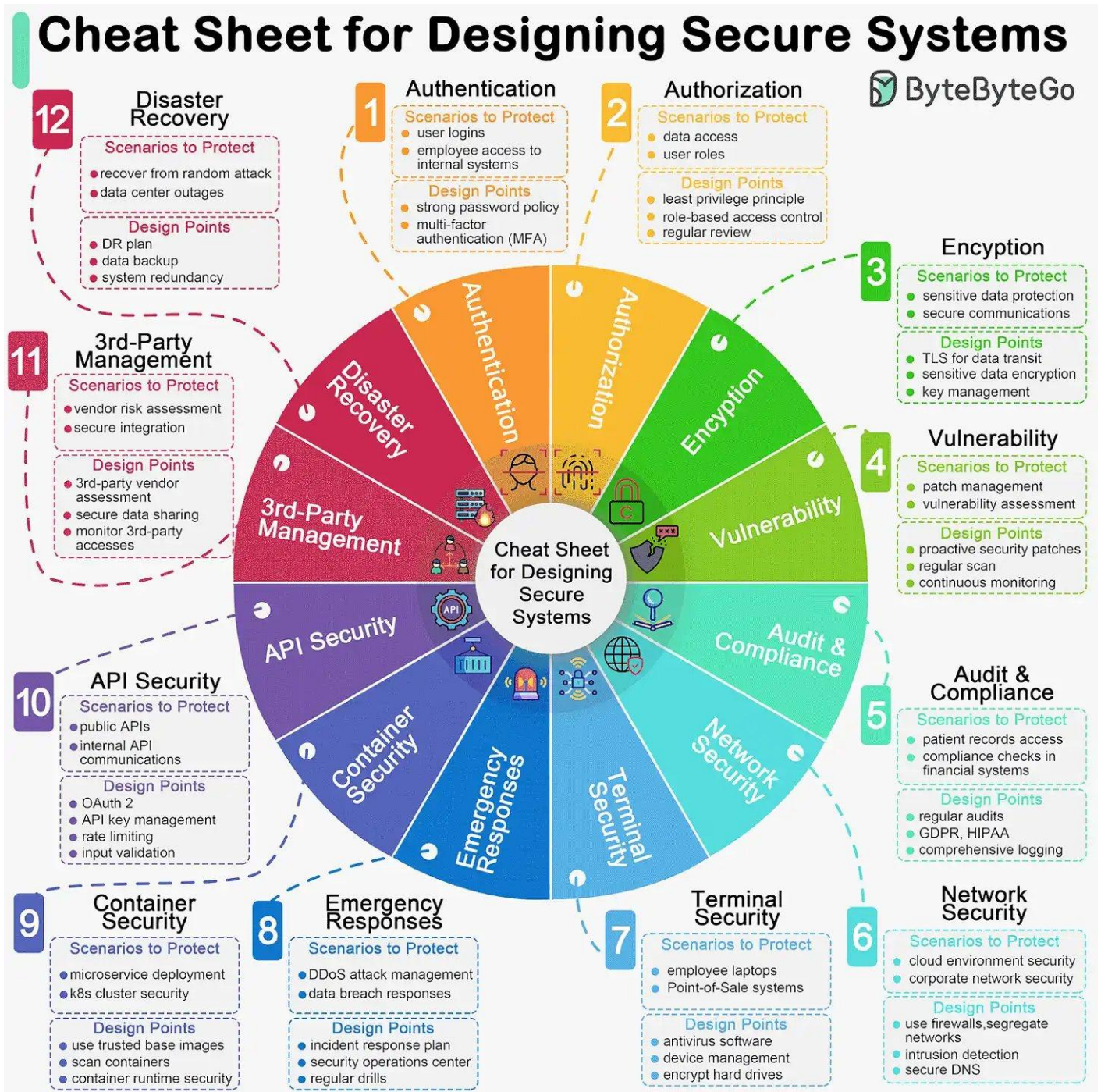
## Credential Stuffing:

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





## Designing Secure Systems



## Risk Management Framework



## Domain 1: Security & Risk Management

## CISSP Cheat Sheet Series

### CIA Triad

<b>Confidentiality</b>	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. Note – Encryption (At transit – TLS) (At rest – AES – 256)
<b>Integrity</b>	Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.
<b>Availability</b>	Ensuring timely and reliable access to and use of information by authorized users.

\*Citation: <https://www.isc2.org/Certifications/CISSP/CISSP-Student-Glossary>

### D.A.D.

<b>Disclosure</b>	<b>Alteration</b>	<b>Destruction</b>
Opposite of Confidentiality	Opposite of Integrity	Opposite of Availability

### Plans

Type	Duration	Example
<b>Strategic Plan</b>	up to 5 Years	Risk Assessment
<b>Tactical Plan</b>	Maximum of 1 year	Project budget, staffing etc
<b>Operational Plan</b>	A few months	Patching computers Updating AV signatures Daily network administration

### Risk Management

- No risk can be completely avoided .
- Risks can be minimized and controlled to avoid impact of damages.
- Risk management is the process of identifying, examining, measuring, mitigating, or transferring risk

\*Citation: <https://resources.infosecinstitute.com/category/certifications-training/cissp/domains/security-and-risk-management/>

**Solution** – Keep risks at a tolerable and acceptable level.  
**Risk management constraints** – Time, budget

### Achieving CIA - Best Practices

Separation of Duties	Mandatory Vacations	Job Rotation	Least Privileges	Need to know	Dual Control
----------------------	---------------------	--------------	------------------	--------------	--------------

#### Availability Measuring Metrics

RTO/MTD/RPO, MTBF, SLA

### IAAAA

<b>Identification</b>	Unique user identification
<b>Authentication</b>	Validation of identification
<b>Authorization</b>	Verification of privileges and permissions for authenticated user
<b>Accountability</b>	Only authorized users are accessing and use the system accordingly
<b>Auditing</b>	Tools, processes, and activities used to achieve and maintain compliance

### Protection Mechanisms

Layering	Abstractions	Data Hiding	Encryption
----------	--------------	-------------	------------

### Data classification

Entails analyzing the data that the organization retains, determining its importance and value, and then assigning it to a category.

### Risk Terminology

<b>Asset</b>	Anything of value to the company.
<b>Vulnerability</b>	A weakness; the absence of a safeguard
<b>Threat</b>	Things that could pose a risk to all or part of an asset
<b>Threat Agent</b>	The entity which carries out the attack
<b>Exploit</b>	An instance of compromise
<b>Risk</b>	The probability of a threat materializing

\*Citation: <https://resources.infosecinstitute.com/category/certifications-training/cissp/domains/security-and-risk-management/>

### Risk Management Frameworks

Preventive Ex ISO 27001	Deterrent Ex ISO 27000	Detective	Corrective	Recovery
Security Policies	Security Personnel	Logs	Alarms	Backups
Security Cameras	Guards	Security Cameras	Antivirus Solutions	Server Clustering
Callback	Security Cameras	Intrusion Detection Systems	Intrusion Detection Systems	Fault Tolerant Drive Systems
Security Awareness Training	Separation of Duties	Honey Pots	Business Continuity Plans	Database Shadowing
Job Rotation	Intrusion Alarms	Audit Trails		Antivirus Software
Encryption	Awareness Training	Mandatory Vacations		
Data Classification	Firewalls			
Smart Cards	Encryption			

### Risk Management Life Cycle

Assessment	Analysis	Mitigation / Response
Categorize, Classify & Evaluate Assets	Qualitative vs Quantitative	Reduce, Transfer, Accept
<b>as per NIST 800-30:</b>	Qualitative – Judgments	Reduce / Avoid
System Characterization	Quantitative – Main terms	Transfer
Threat Identification	AV – Asset Value	Accept / Reject
Vulnerability Identification	EF – Exposure Factor	
Control Analysis	ARO – Annual Rate of Occurrence	
Likelihood Determination	Single Loss Expectancy = AV * EF	

### Security Governance

### Risk Framework Types

Security and Risk Management
Asset Security
Security Engineering
Communications and Network Security
Identity and Access Management
Security Assessment and Testing
Security Operations
Software Development Security

### The 6 Steps of the Risk Management Framework

#### Categorize

#### Select

