Printed by: shikridat@gmail.com. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

Identity and Access	amework				
Management (IAM) is a framework that consists of	Access Management				
users, procedures, and software products to manage	Authentication	Authorization			
user digital identities and access the resources of an	Single Sign on Session Management	Role-based Authorization Authorization			
organization	Password Strong Services Authentication	Artificate based Remote Authorization Authorization			
lt ensures that "the right users obtain access to the right	Multi-factor Authentication				
information at the right time" The services provided by IAM	V	AM User Management			
are classified into four distinct components:	Enterprise Directory Service	Delegated Administration User & Role Management			
Authentication	Senior Sundannination	Provisioning Password Management			
Authorization	Meta Virtual Directory Directory	Self-Service Compliance Auditing			
User Management Enterprise Directory Services					
(Central User Repository)	Identity N	Management			
Authorization Involuted but of the countries of the count	res validating the identity of an individual (E.g. res controlling an individual's access of information overwrite or delete it) thou of keeping track of user actions on the new fuser access to the network. It helps to identify	nation for (E.g., a user can read the file			
	Ĉ.				
		Copyright © by ES-Cossell. All Rights Reserved. Reproduction is Strictly Prohibited.			
otes:					

Printed by: shikridat@gmail.com. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

Types of Authentication: Password Authentication





Password Authentication uses a combination of username and password to authenticate network



The password is checked against a database and allows access, if it matches



Password authentication can be vulnerable to password cracking attacks such as brute force or dictionary attacks

Copyright © by ES-Council. All Rights Reserved. Reproduction is Strictly Prohibited

Types of Authentication: Two-factor Authentication





Two-factor authentication involves using two different authentication factors out of a possible three (a knowledge factor, a possession factor, and an inherence factor) to verify the identity of an individual in order to enhance security in authentication systems



Combinations of two-factor authentication: password and smartcard or token, password and biometrics, password and OTP, smartcard or token and biometrics, or other combinations



Inherence factor (biometric authentication) is the best companion of two-factor authentication as it is considered to be the hardest to forge or spoof



The most widely used physical or behavioral characteristics to establish or verify an identity include fingerprints, palm pattern, voice or face pattern, iris features, keyboard dynamics, and signature dynamics, among others

Copyright $\, \mathfrak{S} \,$ by \mathfrak{W} -Cosscil. All Rights Reserved. Reproduction is Strictly Problemed.

Notes:	 	 	 	 	

Appendix B Page 3702

Ethical Hacking and Countermeasures Copyright © by **EC-Council**All Rights Reserved. Reproduction is Strictly Prohibited.