PASSWORD AUTHENTICATION and VULNERABILITIES Module 2

Password Authentication

SUMMERY

Matched Branch:	0
Partially Matched Branch:	1
Mismatched Branch:	11
Extra Branch:	0
Total Match:	16.22 %
Concept Match:	20.83 %
Link. Phr. Match:	7.69 %
Misconception:	100.0 %
Hierarchy Match:	0.89 %

Grade: 5.66%

expressed by

widely used line of defense against intruders

utilizes

the user ID

determines

user is authorized to access the system

user's privileges, such as root or guest

use in discretionary access control

has the process of

system compares password with the one stored for that specified login

user provides name/login and password

affected by

Types of Vulnerabilities in Passwords

examples of

Offline Dictionary Attack

specified by

Attacker obtains the system password file and compares the password hashes against the hashes of commonly used passwords

Specific Account Attack

recounted by

Attacker guesses password until the correct password is discovered

Exploitation of User Mistakes

represented by

Attacker exploits user mistakes when the system assigns a password for the user, then the user is more likely to write it down due to its inherent difficulty

Electronic Monitoring

distinguished by

Attacker uses electronic monitoring for eavesdropping, thereby exploiting the vulnerability when a password is communicated across the network to log onto a remote system

Exploiting Multiple Password Use

interpreted by

Attacker exploits multiple password use given that attacks can become more effective or damaging if different network devices share thew same or similar password for a given user

Workstation Hijacking

outlined by

Attacker waits until a logged-in workstation is unattended and then hijacks it

Password Guessing

depicted by

Attacker attempts to gain knowledge about the account holder and system password policies and uses that knowledge to guess the password