

Password Authentication

SUMMERY	
Matched Branch:	0
Partially Matched Branch:	12
Mismatched Branch:	0
Extra Branch:	45
Total Match:	27.03 %
Concept Match:	41.67 %
Link. Phr. Match:	0.0 %
Misconception:	100.0 %
Hierarchy Match:	40.67 %

Grade: 22.75%

expressed by

affected by

widely used line of defense against intruders

Types of Vulnerabilities in Passwords

utilizes

has the process of

examples of

the user ID

system compares password with the one stored for that specified login

user provides name/login and password

Offline Dictionary Attack

Specific Account Attack

Exploitation of User Mistakes

Electronic Monitoring

Exploiting Multiple Password Use

Workstation Hijacking

Password Guessing

determines

specified by

recounted by

represented by

distinguished by

interpreted by

outlined by

depicted by

user is authorized to access the system

user's privileges, such as root or guest

use in discretionary access control

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

Attacker guesses password until the correct password is discovered

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

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

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

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

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