Practice test 16

Tuesday, October 24, 2023 4:21 PM

flood guard = feature on circuit-level firewall that prevents malicious connections from forming

data masking = "redacting and substituting character strings"
tokenization = "all or part of data is replaced with randomly generated token"

weak encryption = brute force

account permissions = file perms
access policies = right to log on to pc, install software, change net configs, etc.

SIEM is heavily dependent on data inputs to provide meaningful info about events and trends
    ex: CVE

kerberos
    application server = verify authorization = ACL + session key and service ticket
    KDC server = connectivity = time sync + port 88
    client = verify user creds = time sync + password/pin