ATT&CK

Question 1) Your company heavily relies on cloud services like Azure AD, and Office 365 publicly. What technique should you focus on mitigating, to prevent an attacker performing Discovery activities if they have obtained valid credentials ?

Answer : It's Discovery Tactics (Cloud Service Dashboard)

Question 2) You were analyzing a log and found uncommon data flow on port 4050. What APT group might this be ?

Answer : Search 4050 (G0099)

Question 3) The framework has a list of 9 techniques that falls under the tactic to try to get into your network. What is the tactic ID ?

Answer : This is Initial Access

Question 4) A software prohibits users from accessing their account by deleting, locking the user account, changing password etc. What such software has been documented by the framework ?

Answer : Search LockerGoga

Question 5) Using 'Pass the Hash' technique to enter and control remote systems on a network is common. How would you detect it in your company ?

Answer :

DS0028	Logon Session	Logon Session Creation	Monitor newly created logons and credentials used in events and review for discrepancies. Unusual remote logins that correlate with other suspicious activity (such as writing and executing binaries)