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? (Hint: Not using an API to interact with the cloud environment!)

**T1538**

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

**G0099**

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?

**TA001**

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?

**S0372**

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?

**Audit all logon and credential use events and review for discrepancies.**