ATT&CK

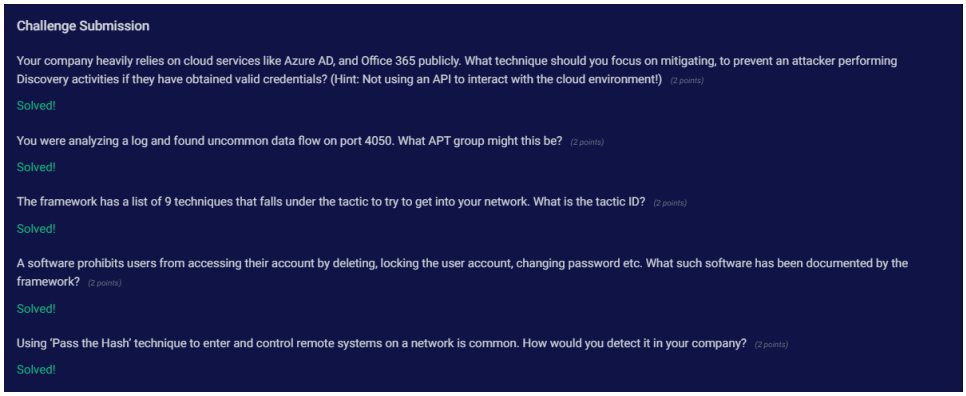
Platform: blueteamlabs.online

Frome: Asem Reda

Diploma: Cybersecurity 87

Challenge link: https://blueteamlabs.online/home/challenge/attck-0e4914db5d

Scenario:You are hired as a Blue Team member for a company. You are assigned to perform threat intelligence for the company. See how you can operationalize the MITRE ATT&CK framework to solve these scenario-based problems.



Task1:

Solution steps:

Open MITRE ATT&CK

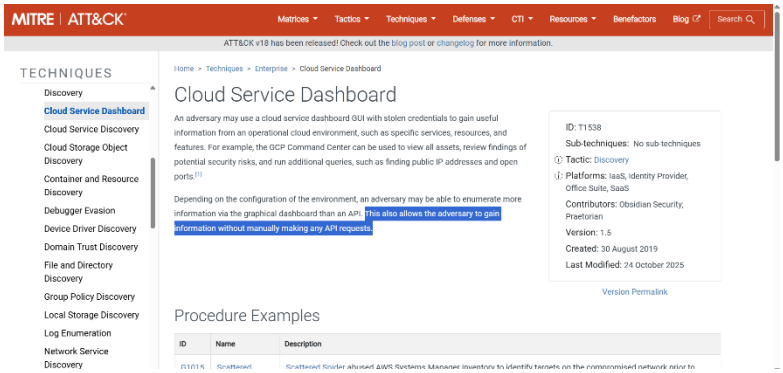
Select Techniques → Enterprise → Cloud

Under Discovery, search for each technology individually

The only one that mentions: **“without making API requests"**

She:

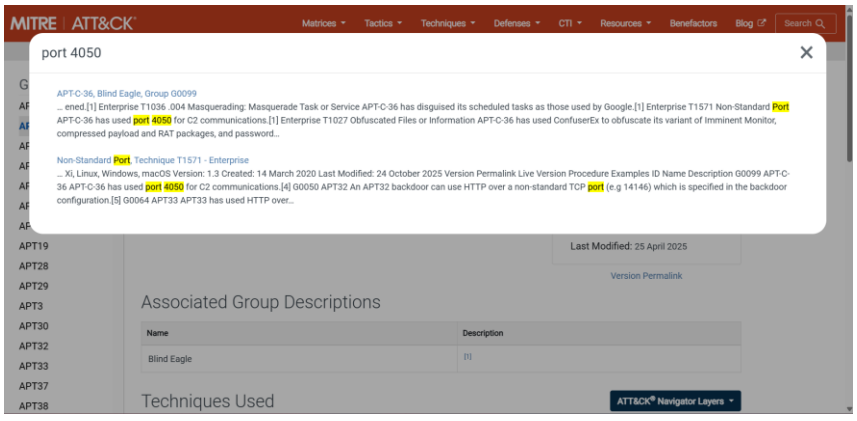
T1538 – Cloud Service Dashboard



Task 2:

Solution steps:

Go to CTI, then select Groups, then type port 4050 in the search bar. You will find the group name G0099 — APT-C-36



Task 3:

Solution steps:

The question states:

"The framework has a list of techniques that fall under the tactic where the adversary is trying to get into your network"

Focusing on the phrase:

"trying to get into your network"

This means: The attacker is still outside the network... and still trying to get in

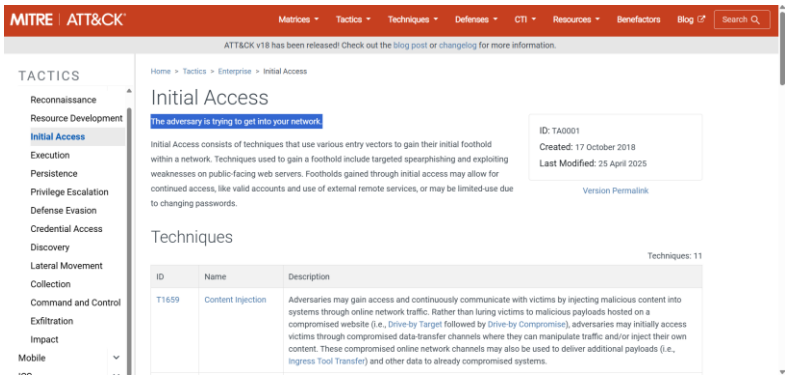
This stage is **Initial Access** because its goal is to attempt to gain access to the network

The text within MITRE confirms this

If you open the MITRE website to Initial Access, you will find the following

"The adversary is trying to get into your network"

This is the same sentence as the question



Task4:

Solution steps:

First, we must identify the technique that describes this behavior, and then we can see which program uses this technique.

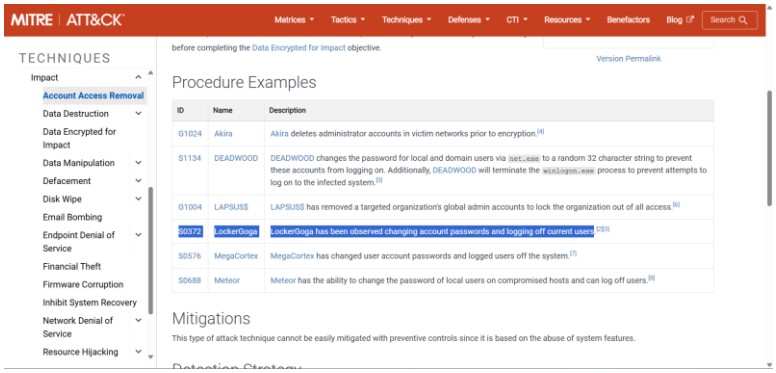
Next, go to the Techniques menu and select Enterprise.

In the search bar, enter keywords like "deleted" and "locked," similar to those mentioned in the question.

Select T1531 because its description matches the question.

Then, scroll down to the Procedure Examples section and you'll find that **"S0372**

LockerGoga has been observed changing account passwords and logging off current users"



Task 5:

First, type "Pass the Hash" in the search bar, then select "Detection Strategy for T1550.002 - Pass the Hash (Windows), Detection Strategy DET0409." Next, scroll down to "Analytics Windows AN1144" and read the text. You will find that the answer is **"Monitor newly created logons and credentials used in events and review for discrepancies"**

Summary of the pass the hash page:

It tells you to:

1. Monitor for unusual NTLM logins

2. Monitor for new Logon sessions

3. Monitor if the user is logging into an unusual machine

4. Interrelate all of this information 5. Use Windows + Sysmon events for detection