

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.

Challenge Submission

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!) (2 points)

Solved!

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

Solved!

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? (2 points)

Solved!

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? (2 points)

Solved!

Using 'Pass the Hash' technique to enter and control remote systems on a network is common. How would you detect it in your company? (2 points)

Solved!

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

The screenshot shows the MITRE ATT&CK interface. The top navigation bar includes links for Members, Tactics, Techniques, Defenses, CTI, Resources, Benefactors, Blog, and Search. A message at the top states: "ATT&CK v18 has been released! Check out the blog post or changelog for more information." The main content area is titled "Cloud Service Dashboard". On the left, there's a sidebar with a "TECHNIQUES" section containing various discovery techniques like Cloud Service Discovery, Cloud Storage Object Discovery, Container and Resource Discovery, Debugger Evasion, Device Driver Discovery, Domain Trust Discovery, File and Directory Discovery, Group Policy Discovery, Local Storage Discovery, Log Enumeration, Network Service Discovery, and others. The central panel displays the details for T1538: "Cloud Service Dashboard". It describes how an adversary can use a cloud service dashboard GUI with stolen credentials to gain useful information from an operational cloud environment. It notes that the GCP Command Center can be used to view all assets, review findings of potential security risks, and run additional queries, such as finding public IP addresses and open ports.^[1] Depending on the configuration of the environment, an adversary may be able to enumerate more information via the graphical dashboard than an API. This also allows the adversary to gain information without manually making any API requests. The right side of the panel shows the technique's ID (T1538), sub-techniques (none), tactic (Discovery), platforms (IaaS, Identity Provider, Office Suite, SaaS), contributors (Obdian Security, Praetorian), version (1.5), creation date (30 August 2019), and last modified date (24 October 2025). A "Version Permalink" link is also present.

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

The screenshot shows the MITRE ATT&CK interface with a search bar at the top containing "port 4050". The results are displayed in a modal window. The first result is "G APT-C-36, Blind Eagle, Group: G0099", which is described as "..._emed.[1] Enterprise T1036 - 204 Masquerading: Task or Service APT-C-36 has disguised its scheduled tasks as those used by Google.[1] Enterprise T1571 Non-Standard Port APT-C-36 has used port 4050 for C2 communications.[1] Enterprise T1027 Obfuscated Files or Information APT-C-36 has used ConfuserEx to obfuscate its variant of Imminent Monitor, compressed payload and RAT packages, and password...". Below this, there are other entries: "Non-Standard Port, Technique T1571 - Enterprise ..._X, Linux, Windows, macOS Version: 1.3 Created: 14 March 2020 Last Modified: 24 October 2025 Version Permalink Live Version Procedure Examples ID Name Description G0099 APT-C-36 APT-C-36 has used port 4050 for C2 communications [4] G0050 APT32 An APT32 backdoor can use HTTP over a non-standard TCP port (e.g 14146) which is specified in the backdoor configuration [5] G0064 APT33 APT33 has used HTTP over...". The modal also shows "Associated Group Descriptions" for "Blind Eagle" and "Techniques Used" for "Blind Eagle". The bottom right corner of the modal has a "Version Permalink" link.

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

The screenshot shows the MITRE ATT&CK website. The navigation bar includes 'Matrices', 'Tactics', 'Techniques', 'Defenses', 'CTI', 'Resources', 'Benefactors', 'Blog', and a search bar. The main content area is titled 'Initial Access' with the sub-section 'Reconnaissance'. A callout box highlights the text: 'The adversary is trying to get into your network'. Below this, a detailed description of Initial Access is provided. To the right, there is a box containing the ID: TA0001, Created: 17 October 2018, and Last Modified: 25 April 2025. At the bottom of the page, there is a section titled 'Techniques' with a table listing one technique: T1659 Content Injection.

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**

Data Component	Name	Channel
Logon Session Creation (DC0067)	WinEventLog Security	EventCode=4624, 4648
Active Directory Credential Request (DC0084)	WinEventLog Security	EventCode=4768
Network Connection Creation (DC0082)	WinEventLog Sysmon	EventCode=3, 22
Process Creation (DC0032)	WinEventLog Sysmon	EventCode=1