

ATT&CK-Blueteam lab

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.

Q1. 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!)

answer/T1538

Description

The adversary attempts to gain an initial foothold within the target environment

TACTICS			within a cloud service provider or SaaS application.
Resource Development	T1010	Application Window Discovery	Adversaries may attempt to get a listing of open application windows. Window listings could convey information about how the system is used. For example, information about application windows could be used identify potential data to collect as well as identifying security tooling (Security Software Discovery) to evade.
Initial Access	T1217	Browser Information Discovery	Adversaries may enumerate information about browsers to learn more about compromised environments. Data saved by browsers (such as bookmarks, accounts, and browsing history) may reveal a variety of personal information about users (e.g., banking sites, relationships/interests, social media, etc.) as well as details about internal network resources such as servers, tools/dashboards, or other related infrastructure.
Execution	T1580	Cloud Infrastructure Discovery	An adversary may attempt to discover infrastructure and resources that are available within an infrastructure-as-a-service (IaaS) environment. This includes compute service resources such as instances, virtual machines, and snapshots as well as resources of other services including the storage and database services.
Persistence	T1538	Cloud Service Dashboard	An adversary may use a cloud service dashboard GUI with stolen credentials to gain useful information from an operational cloud environment, such as specific services, resources, and features. For example, 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.
Privilege Escalation	T1526	Cloud Service Discovery	An adversary may attempt to enumerate the cloud services running on a system after gaining access. These methods can differ from platform-as-a-service (PaaS), to infrastructure-as-a-service (IaaS), or software-as-a-service (SaaS). Many services exist throughout the various cloud providers and can include Continuous Integration and Continuous Delivery (CI/CD), Lambda Functions, Entra ID, etc. They may also include security
Defense Evasion			
Credential Access			
Discovery			
Lateral Movement			
Collection			
Command and Control			
Exfiltration			
Impact			
Mobile			

Q2-You were analyzing a log and found uncommon data flow on port 4050. What APT group might this be? Answer/G0099

Port **4050** is a non-standard network port commonly abused by attackers for **Command and Control (C2) communication**. It has been observed in APT activity to maintain remote access, evade detection, and exchange malicious commands between compromised systems and attacker servers.

The screenshot shows a browser window with the URL attack.mitre.org/techniques/enterprise/. The search bar at the top contains the query "port 4050". Below the search bar, there is a list of techniques. The first item in the list is "APT-C-36, Blind Eagle, Group G0099". The description for this technique includes the sentence "... ened.[1] Enterprise T1036 .004 Masquerading: Masquerade 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..." with the word "port 4050" highlighted in yellow.

Q3-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/TA001

Initial Access (TA0001) refers to the techniques attackers use to gain their first entry into a target environment. This includes methods such as phishing, exploiting public-facing applications, brute-force attacks, or using stolen credentials to establish an initial foothold in the network.

The screenshot shows a browser window with the URL attack.mitre.org/tactics/TA0001/. The left sidebar is titled "TACTICS" and lists several categories: Reconnaissance, Resource Development, **Initial Access**, Execution, Persistence, Privilege Escalation, and Defense Evasion. The "Initial Access" category is currently selected. The main content area shows the title "Initial Access" and a brief description: "The adversary is trying to get into your network." Below this, there is a detailed description of the tactic: "Initial Access consists of techniques that use various entry vectors to gain their initial foothold within a network. Techniques used to gain a foothold include targeted spearphishing and exploiting weaknesses on public-facing web servers. Footholds gained through initial access may allow for continued access, like valid accounts and use of external remote services, or may be limited-use due to changing passwords." To the right of the description, there is a box containing the tactic's metadata: "ID: TA0001", "Created: 17 October 2018", and "Last Modified: 25 April 2025". At the bottom right of the page, there is a link "Version Permalink".

Q4-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/S0372

Account Access Removal (T1531) is an impact technique where attackers delete user accounts or change account passwords to block legitimate users from accessing their systems. This is commonly used to disrupt operations, delay incident response, and maintain attacker control over the environment.

The screenshot shows the MITRE ATT&CK website with the URL attack.mitre.org/techniques/T1531/. The left sidebar under 'TECHNIQUES' has 'Account Access Removal' selected. The main content area displays a table of procedure examples:

ID	Name	Description
G1024	Akira	Akira deletes administrator accounts in victim networks prior to encryption. ^[4]
S1134	DEADWOOD	DEADWOOD changes the password for local and domain users via <code>net.exe</code> to a random 32 character string to prevent these accounts from logging on. Additionally, DEADWOOD will terminate the <code>winlogon.exe</code> process to prevent attempts to log on to the infected system. ^[5]
G1004	LAPSUS\$	LAPSUS\$ has removed a targeted organization's global admin accounts to lock the organization out of all access. ^[6]
S0372	LockerGoga	LockerGoga has been observed changing account passwords and logging off current users. ^{[2][3]}
S0576	MegaCortex	MegaCortex has changed user account passwords and logged users off the system. ^[7]

Q5-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/Monitor newly created logons and credentials used in events and review for discrepancies

The screenshot shows the MITRE ATT&CK website with the URL attack.mitre.org/techniques/T1550/. The left sidebar under 'TECHNIQUES' has 'Pass the Ticket' selected. The main content area displays the title 'Use Alternate Authentication Material: Pass the Ticket' and a detailed description of the technique:

Adversaries may "pass the ticket" using stolen Kerberos tickets to move laterally within an environment, bypassing normal system access controls. Pass the ticket (PtT) is a method of authenticating to a system using Kerberos tickets without having access to an account's password. Kerberos authentication can be used as the first step to lateral movement to a remote system.

When performing PtT, valid Kerberos tickets for Valid Accounts are captured by OS Credential Dumping. A user's service tickets or ticket granting ticket (TGT) may be obtained, depending on the level of access. A service ticket allows for access to a particular resource, whereas a TGT can be used to request service tickets from the Ticket Granting Service (TGS) to access any resource the user has privileges to access.^{[1][2]}

A Silver Ticket can be obtained for services that use Kerberos as an authentication mechanism and

On the right side, there is a box with the following details:

- ID: T1550.003
- Sub-technique of: T1550
- Tactics: Defense Evasion, Lateral Movement
- Platforms: Windows
- Contributors: Ryan Becwar, Vincent Le Toux
- Version: 1.2
- Created: 30 January 2020
- Last Modified: 24 October 2025