IAM, or Identity and Access Management, is like the bouncer at a party who decides who gets in and what they're allowed to do once they're inside.

Authentication

**Authentication:** Authentication is the process of verifying your identity. It ensures that you are who you claim to be. credentials, such as a username and password, fingerprint, or security token, uba keys

Authorization

What you are permitted to access, the actions that you can do in the envirnment

IAM is like the gatekeeper of digital systems, managing who can enter, what they can do, and keeping everything safe and secure

Just like the bouncer ensures only authorized people enter the party to prevent trouble, IAM helps protect sensitive information and resources from unauthorized access or misuse by controlling who has access to what.

OKTA – IAM tool

Okta provides cloud-based identity management solutions that enable organizations to securely manage and authenticate users across various applications, devices, and services.

Okta is like a master key that helps you access all the different rooms (applications and services) you use online with just one key (username and password). It helps keep your digital life organized and secure by managing your logins and ensuring only the right people get access to the right places.

**Universal Directory:** Okta's Universal Directory provides a centralized repository for storing and managing user identities, groups, and attributes, allowing for consistent access control policies across applications.

Lifecycle: onboarding provisioning updates changes, deactivation, automation of user lifecylce

Understand logs

s/m log

eventypes explain

user account hijack

1. **Phishing:** Scenario: An employee receives an email purportedly from their company's IT department, claiming there's been a security breach and urging them to click a link to reset their password immediately. The email looks convincing, with the company's logo and email format. Explanation: In this scenario, the attacker sends a deceptive email (phishing) pretending to be a legitimate entity to trick the user into disclosing their credentials. Clicking the link could lead to a fake website designed to steal login information.
2. **Credential Stuffing:** Scenario: A hacker obtains a list of usernames and passwords from a data breach on a popular social media platform. They then use automated tools to try these same username/password combinations on various other websites, such as online banking or e-commerce sites. Explanation: In this scenario, the attacker exploits the fact that users often reuse the same credentials across multiple platforms. By trying stolen credentials on other websites, they hope to gain unauthorized access to additional accounts through credential stuffing.
3. **Brute Force Attacks:** Scenario: An attacker targets a company's login page and attempts to gain access by systematically trying different combinations of usernames and passwords. They use automated software that can rapidly generate and test thousands of combinations until they find one that works. Explanation: Brute force attacks rely on sheer computing power to try every possible combination of usernames and passwords until the correct one is found. While this method can be time-consuming and resource-intensive, it can be successful if the attacker discovers a weak or easily guessable password.

In all these scenarios, the attackers exploit vulnerabilities in human behavior, system weaknesses, or both, highlighting the importance of robust security measures such as user education, multi-factor authentication, and strong password policies to mitigate the risks associated with these types of attacks.

Password spraying

Password spraying is more focused on trying a few common passwords against many accounts to evade detection, while brute force attacks involve trying every possible password combination against a single account

One good thing about OKTA, it has inbuilt threat detections. So wherever okta thinks security threat . eventtype is . okta categorize them . it has already stopped it which is why it has been logged.

Pass word spray from some ip is already blocked

IF you want to look at trend then checkwhich user agent, location and give a graph for your stakeholdes.

Suspicious tenant takeover

When an adversary successfully compromises an administrator they might try to block access to the rest of the administrators in the organization to strengthen their hold on the tenant and ensure that no one can reverse their actions.

An admin trying to do action on other user account i.e actor performing an action on target.

Target field will be a dictionary where you will have to extract only email id.

Deactivation/suspension of that user account if success, take time frame count unique no

Based on threshold output

So we see a actor with 3 deactivation user. There can be cases where If user goes out

If admin then ok else u have a prob

Admin privilege revoked. (frm admin/gp with admin privilege)

I got access. And I don’t want other admins to interfere. Deactivate/revoke their permissions

It is fine if a system is performing these activities but if its not a system then you have a prob

Threatinsight alert:

OKTA identifies threat and categories

Security threat detected event type

Ligin\_fail in password spray. Okta took care.

Session hijack

Ur session someone else want ur cookie or they have it

How okta tackles is using dehash ddhash

De identification token hash – gives you unique token for a session okta says any session should be limited to 2 hrs if this token is been used by this user. But this token is also used by same user from diff location which doesn’t look good.i.e 2 other attacker from diff countries

More parametes next

Session impersonation:

Suppose the support tam wants to take ur admin access for trbleshooting activity. Ie an impersonation. Usually not many no of events.

But if its unusual increase of events.like loads of events. Something is going one. Event types Initiation then grant. If u don’t see grant but an initiation, that means someone is trying to get session

MFA Push notification fatigue

Like the name

Attacker send floods mfa request user feds up accidentally clicks a yes

Eventtype is sm.p

Policy manipulation.

Attacker wants to delte/update/deactivate/play with rules of policy

Policy downgrade

Authentication policy when attacker makes sure that authentication is easier, so they will downgrade policy. Lifecycle /rule update/additions

Token manipulation

Persistent in mitre framewok. Someone is trying to create or update api token to have access to application

Fastpass- take care of phishing

Interesting eventtypes – read

One exercise – map all these into mitre framework.

User ac – credential access,

Password spraying – “”

Token manipulation – persistence

Session hijack-defense evasion