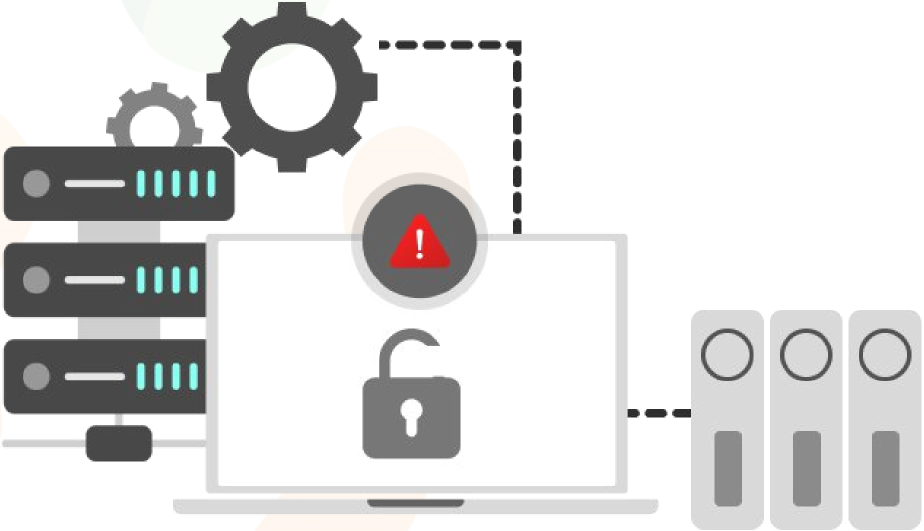
IdentityShield



Unmasking LDAP & KERBEROS Vulnerabilities

miniOrange

AVI SAXENA

SENIOR SOFTWARE ENGINEER

- Experienced on working in LDAP and Kerberos Integration for 3+ Years.
- WordPress Plugin Developer in Cyber Security Domain
- Works on providing solutions for API Security use cases.

EMAIL: *AVI@XECURIFY.COM*

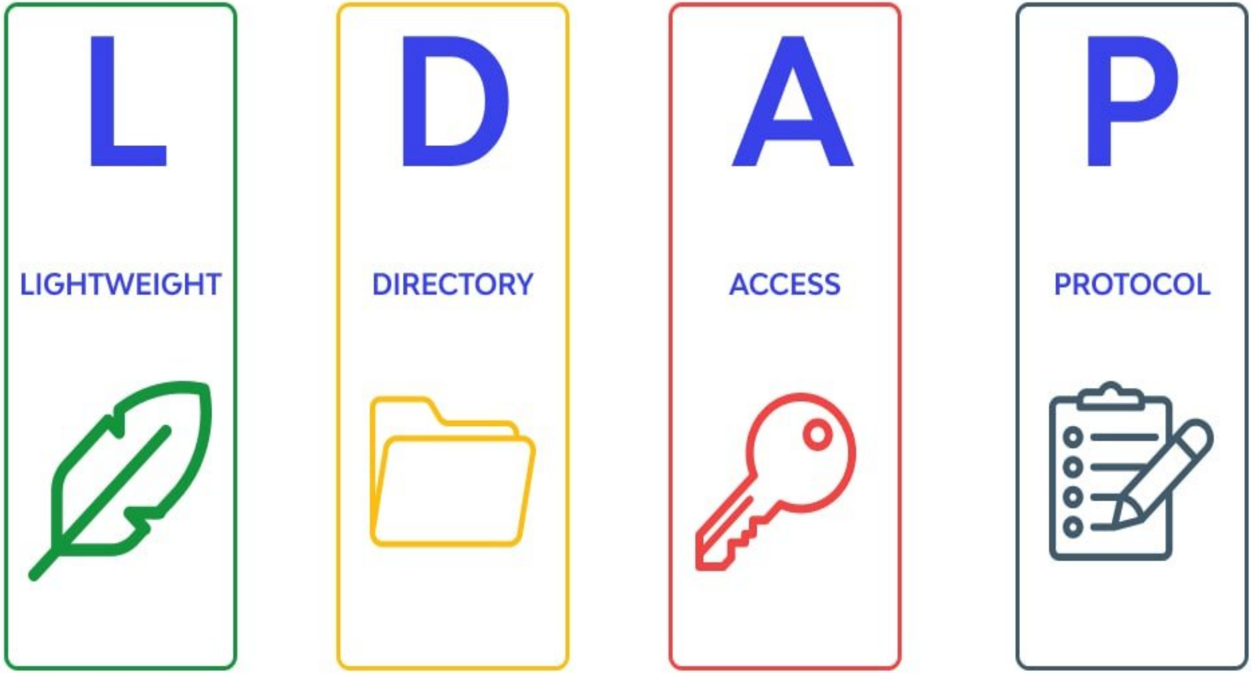
WHO AM I?

WHAT IS A DIRECTORY ?

- A directory is a hierarchical database which can easily mimic an organisation’s structure with information like user objects, computers etc.
- It can be accessed via LDAP that could be used for Authentication & perform CRUD operations.
- Ex: Microsoft Active Directory, FreeIPA, OpenLDAP, ApacheDS, OpenDJ.

IdentityShield

WHAT IS LDAP PROTOCOL ?



L

LIGHTWEIGHT

D

DIRECTORY

A

ACCESS

P

PROTOCOL

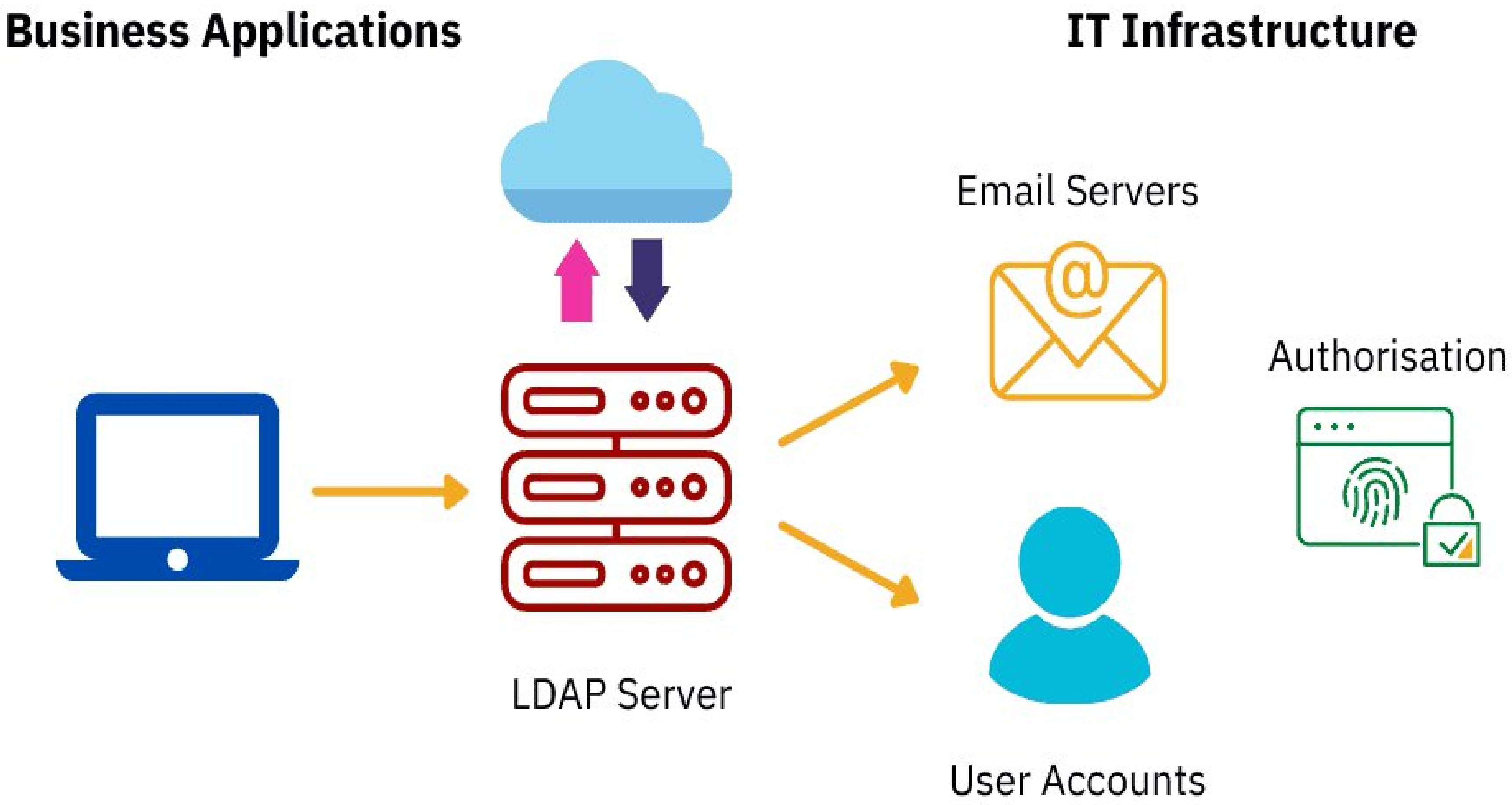
miniOrange

WHAT IS LDAP PROTOCOL ?

- LDAP is used to query into a Directory to Bind, Authenticate users & perform CRUD operations on the objects.
- It can be used to connect to the Directory from outside the network as well.
- Required/Used by 3rd Party Apps to connect their services to their company’s Directory.

Let’s Discuss

WHERE IS A DIRECTORY USED ?



Business Applications

IT Infrastructure

Email Servers

Authorisation

LDAP Server

User Accounts

Meet
~~Fluffy~~
KERBEROS

Unlike Fluffy

MUSIC DOESN’T TAKE KERBEROS DOWN ;)

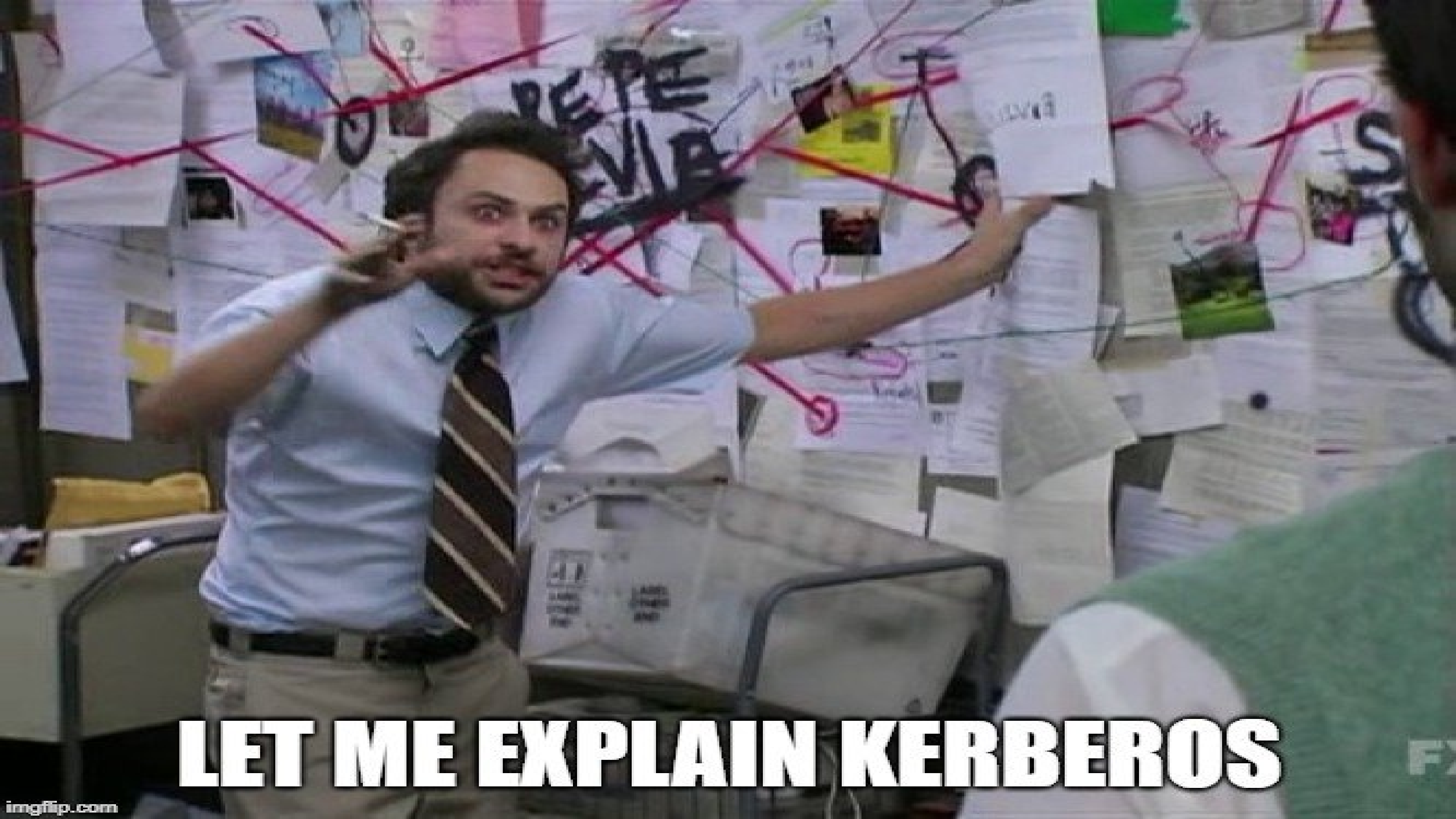
WHAT IS KERBEROS ?

- Kerberos is an authentication protocol typically used by clients in a domain joined network.
- Each domain user have complete access of a workstation, but a workstation cannot be completely trusted to identify its user for accessing any service.
- Kerberos act as a 3rd party authenticator to help users prove their identity for accessing services

WHY TO USE KERBEROS ?

- Authentication is required at multiple steps for multi-user environments, Auto-login plays a crucial role.

- Sending username & password over the network is not always secure, and can lead to the probability of interception.

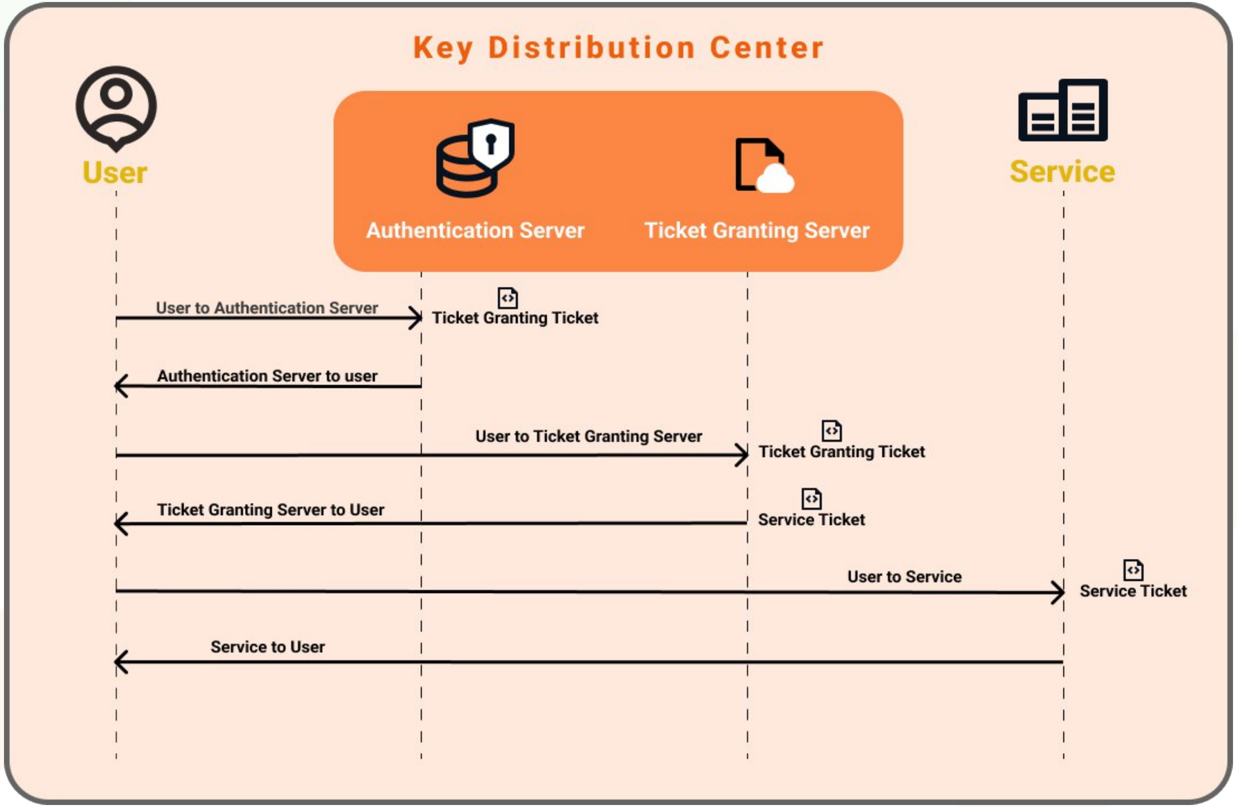


LET ME EXPLAIN KERBEROS
imgflip.com

FEW TERMINOLOGIES TO KNOW

- **CLIENT**: A normal user who wants to access the service.
- **Key Distribution Center (KDC)**: The most important component which plays the main role in Authentication Process.
- **Application Server**: Any Application Service such as SQL.
- **TGT - Ticket Granting Ticket**: Ticket needed for requesting TGS from KDC, It is obtained from the KDC only.
- **TGS - Ticket Granting Service**: Ticket needed for Authenticating against a particular service.
- **SPN - Service Principal Name**: SPN is an identifier for each service instance, it is one of the key Components in the process of authentication.

WORKING OF KERBEROS PROTOCOL



LDAP & KERBEROS VULNERABILITIES

PASSWORD SPRAYING

KERBEROASTING

Pass-the-hash with MIMIKATZ

LDAP INJECTION

1: LDAP INJECTION

- Attackers exploit vulnerabilities in web applications integrated with Active Directory / LDAP Directories to manipulate LDAP queries
- This can lead to unauthorized access to or manipulation of directory services data
- These attacks can compromise the security of an entire network by allowing attackers to bypass authentication, access sensitive information, and even modify directory data

LDAP INJECTION

- **LDAP Search Filter Example:**
    - **Search Filter:** (&(objectclass=user)(samaccountname=<username>))
    - **Correct search filter:**
        - **username=** ”vikas”
        - (&(objectclass=user)(samaccountname=**vikas**))
    - **LDAP Injection Search Filter**
        - **Injected username**: “vikas)(telephonenumber=*”
        - (&(objectclass=user)(samaccountname=vikas)(telephonenumber=*))

DEMO

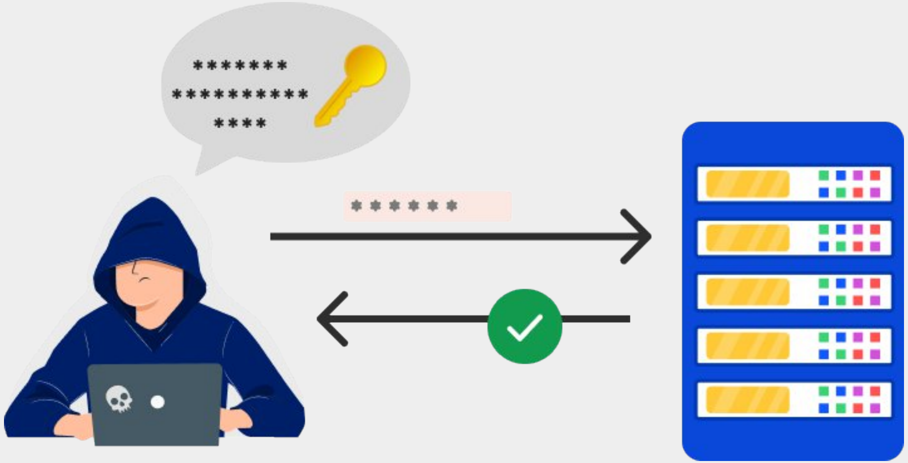
2: PASSWORD SPRAYING

- Password spraying is a type of brute force attack
- It attempts to access multiple user accounts using a few commonly used passwords unlike traditional brute force attacks that focus on one account at a time
- This makes sure the least likelihood of triggering security measures like account lockouts

DEMO

3: PASS-THE-HASH with Mimikatz

- Pass-the-hash is a technique used to steal credentials from Active Directory and also facilitates lateral movement throughout the environment.
- Attackers exploit the NTLM authentication protocol to impersonate a user and dump credential hashes from memory.
- Mimikatz has become the standard tool for exploiting the NTLM authentication protocol.
- Mimikatz extracts the NTLM hashes stored in the local system memory or the Ntds.dit file.



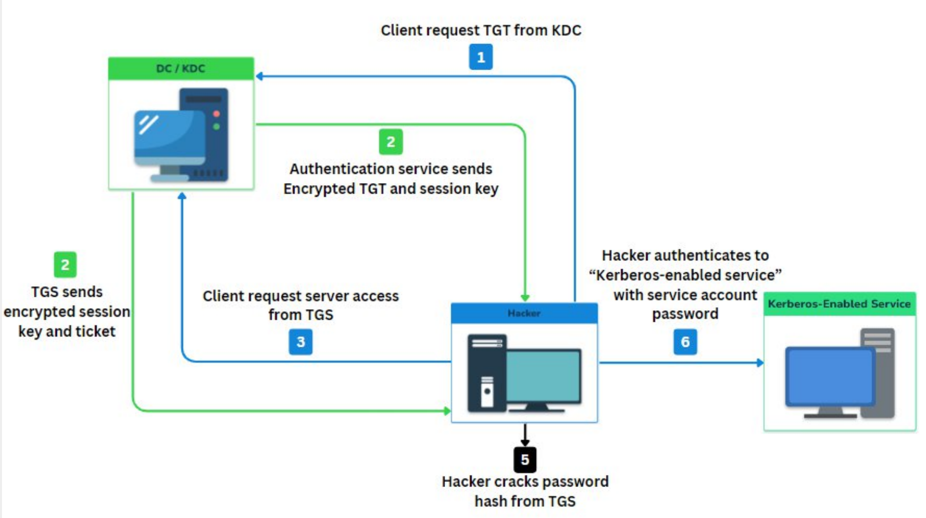
DEMO

4: KERBEROASTING

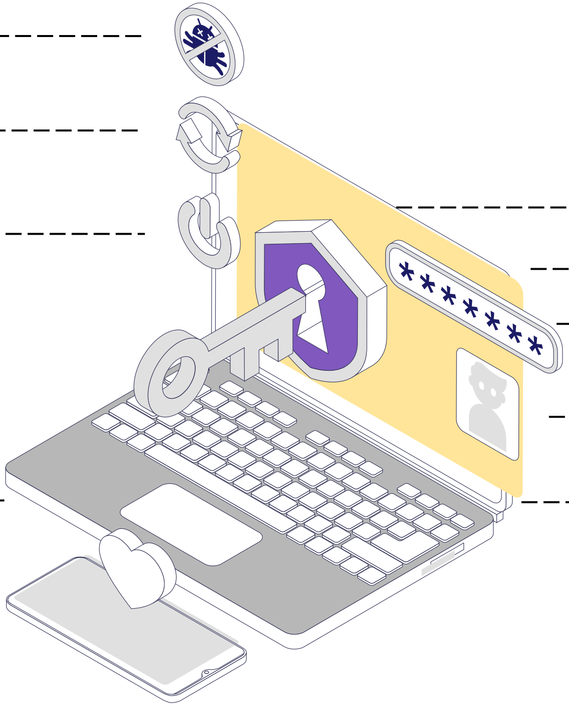
WHAT IS KERBEROASTING?

- Kerberoasting is a type of cyber attack targeting Windows Active Directory environments.
- It exploits the Kerberos protocol Ticket Granting Service (TGS) to crack the passwords of service accounts.
- Service accounts are special user accounts that are created for running applications or services on a network, and they often have elevated privileges.

HOW KERBEROASTING WORKS?



CONSEQUENCES OF ATTACKS



Data Breaches:

Network Compromise

Directory Enumeration & Data Modification

Bypassing Authentication Mechanisms

Unauthorized Access to Sensitive Information

Operational Disruption

Compliance Violations

Financial Impact

Elevated Access and Privilege Escalation

IdentityShield

BEST PRACTICES for Organizations

Strong Password Policies

Monitor and Analyze Login Attempts

Account Lockout Policies

Implement Logon restrictions

Educate and Train Users

Multi-factor Authentication (MFA)

miniOrange

ANY QUESTIONS ?

IdentityShield

miniOrange

Please Submit Your VALUABLE FEEDBACK

THANK YOU