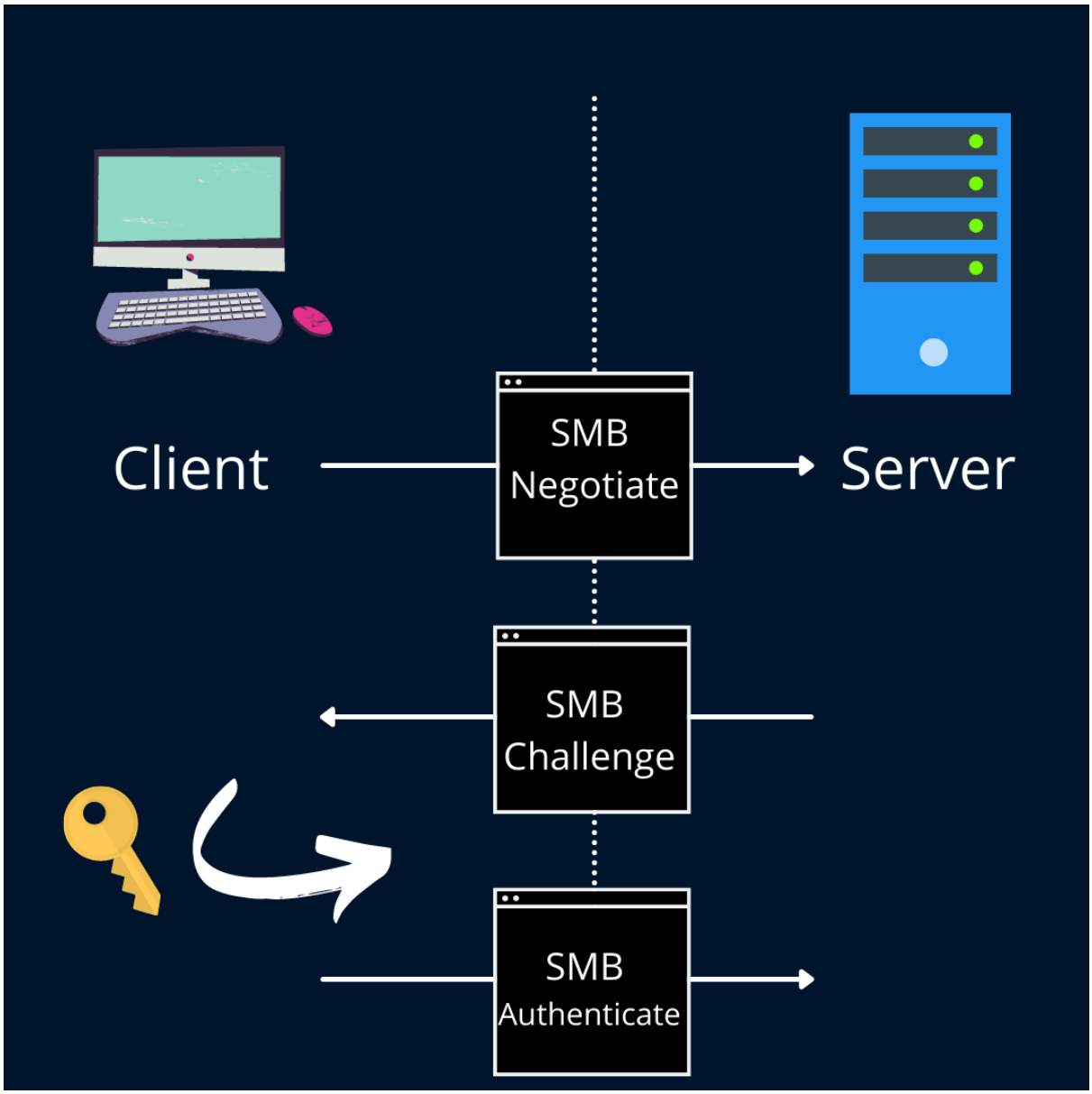
https://blueteamresources.in/ntlm-and-kerberos-authentication/

How does NTLM Authentication work?

NTLM is an authentication protocol in Windows Active Directory. NTLM uses an encrypted challenge-response authentication process to authenticate a user without sending its password over. We know that passwords are stored in Doman Controller in Active Directory. First, the client sends an authentication request called NTLM Negotiate with user details. The Server replies with the NTLM Challenge (a 16-byte number). This number is encrypted with the hashed value of the client's passwords. The server since it stores the passwords, it itself encrypts the challenge with the user password has and compares it with the response. If the values match, the user is authenticated.



How does Kerberos Authentication work?

In Kerberos Authentication for Active Directory, there are multiple servers involved and the security is enhanced compared to NTLM. There is a Key Distribution Centre that manages the password for all accounts which hosts a database and two servers namely the Authentication server and the Ticket granting server. The Authentication server is used to authenticate the user and provide a

ticket (Ticket-granting ticket or TGT) which is verified by Ticket Granting Server and then grants the access to the server. Let's see what exactly happens in a scenario when an internal client wants to access a server (let's say web) in a network.

1) An authentication request is sent to the Authentication server which contains the username, system time, and service information which is encrypted with user password hash.
2) The Authentication server accesses the database that contains the user password hash, decrypts the request and then grants a TGT (Ticket-granting Ticket) to the user which is encrypted with the Key Distribution Centre's (KDC) password hash and the session key required to access the web server which is encrypted with user password hash.
3) Now, the client will send session key and TGT to the Ticket Granting Server (TGS) to acquire the service ticket to access the server.
4) The TGS will check the TGT and decrypt it with KDC Password hash to verify the authenticity of the ticket. If valid, it provides the service ticket to access the server. This service ticket, contains the user password hash encrypted with the web server's password hash. Thus, this can only be decrypted by the server.
5) Now, the user holds a session key and a service ticket. This is sent to the web server.
6) This service ticket is decrypted by the web server with its password hash to find out the user password hash. Then, the user password hash is used to decrypt the session key and then the data communication starts.