SCSP©

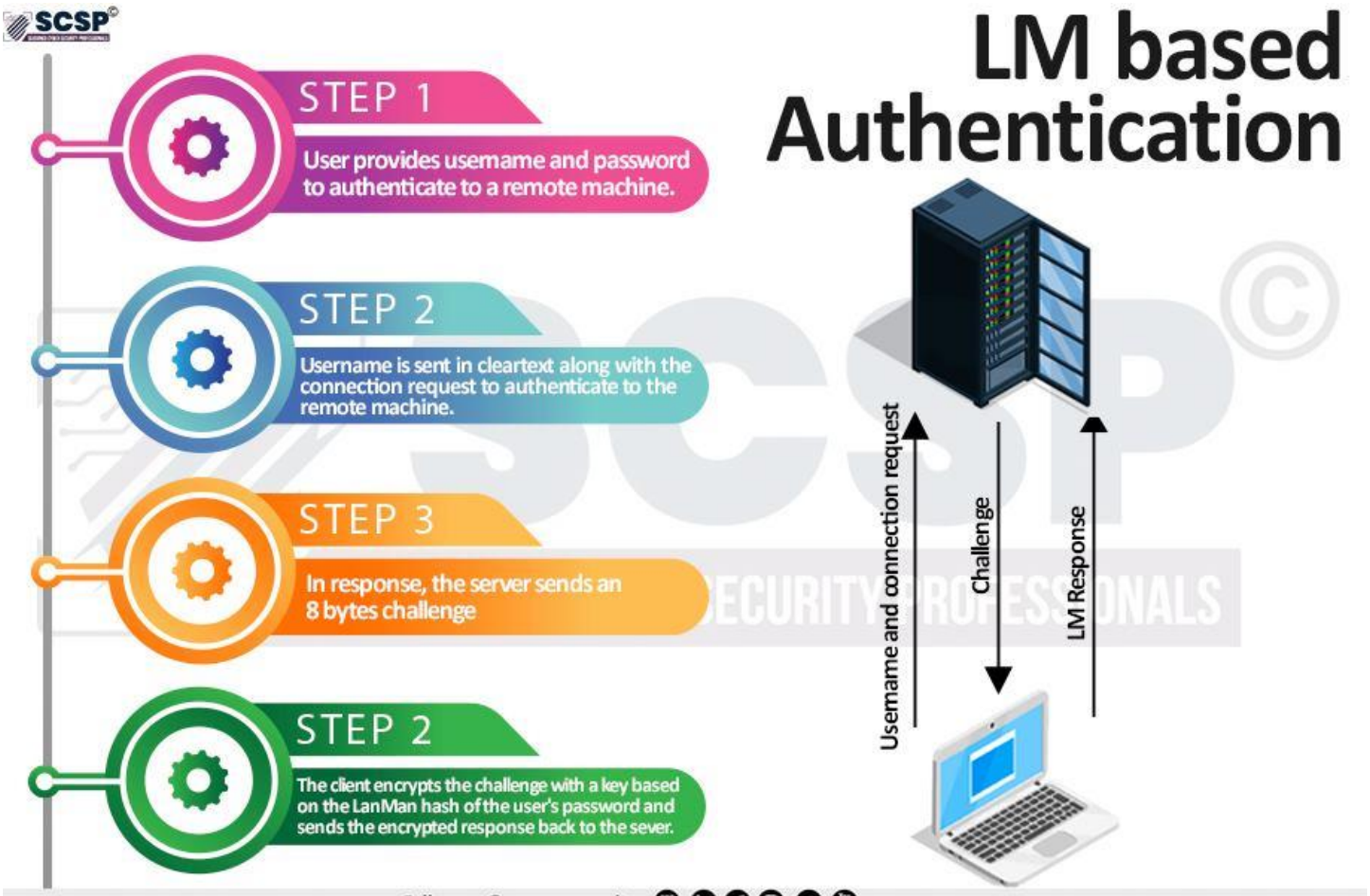
Types of Windows Authentication Mechanisms

Relies on hashes to determine whether a remote user has provided a valid username/password combination.

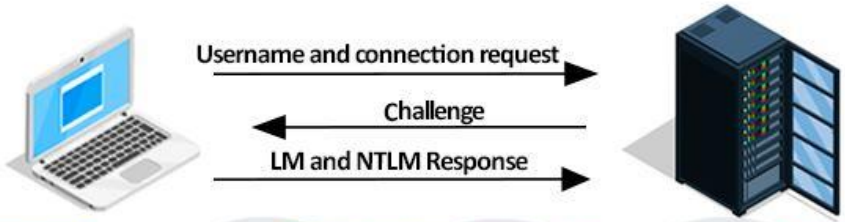
Is calculated across the entire case sensitive password, resulting in a 16-byte hash.

Verification of the user's identity takes place between the domain controller and the client.

LM based Authentication



NTLM based Aunthentication



NTLM is a challenge-response authentication protocol that uses three messages to authenticate a client in a connection oriented environment and a fourth message if integrity is desired.

Client establishes a network path to the server and sends a NEGOTIATE_MESSAGE advertising its capabilities.

Server responds with Challenge_MESSAGE which is used to establish the identity of the client.

Finally, the client responds to the challenge with an AUTHENTICATE_MESSAGE

NTLM protocol uses one or both of the two hashed password values, both of which are also stored on the server and which are password equivalent.

The two are the LM hash and the NT hash, which are 16 bytes each.

KERBEROS based Authentication

Kerberos is a computer network authentication protocol that works on the basis of tickets. It allows nodes that are communicating over an unsecure network to prove their identity.

It is the default auth-mechanism for Microsoft Windows, and has implementations in MAC OS, Linux, FreeBSD etc.