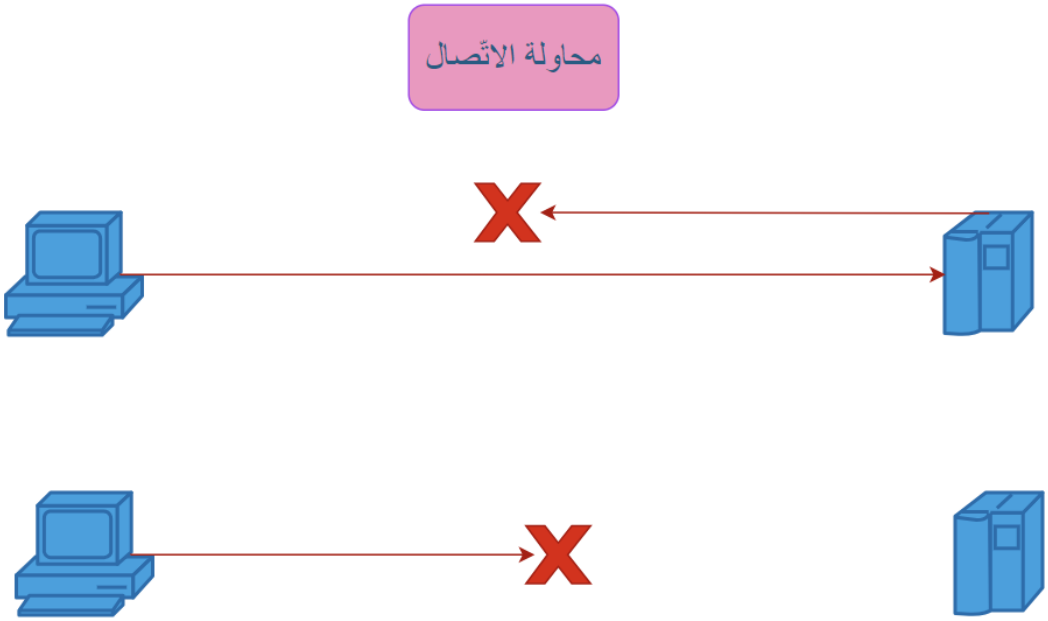
مكوِّنات Nanar C2:

1. **Server** : هو مُخدّم مركزي قادر على الاتِّصال بالعديد من العملاء في آنٍ واحد، وهو المركز الأساسي الَّذي من خلاله يتمُّ إرسال الأوامر إلى العُملاء من أجل التَّنفيذ

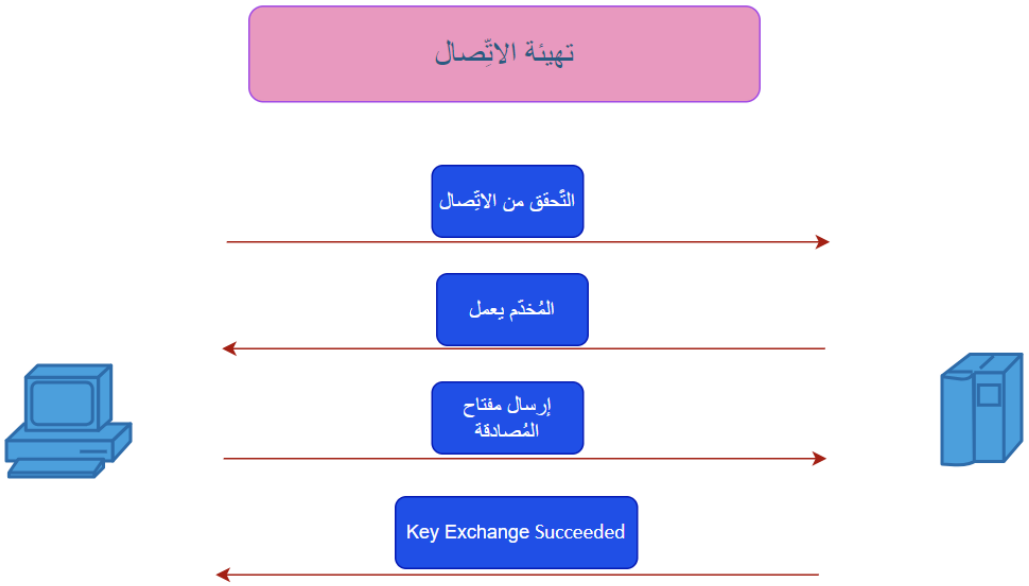
2. **Client** : يتم إيصاله إلى جهاز الهدف، وهو المسؤول عن تنفيذ الإجرائيَّات في جهاز الهدف عن طريق استقبال الأوامر من المُخدِّم، ثُمَّ إرسال النَّتائج إليه.

مراحل الاتِّصال:

1. **محاولة الاتِّصال** : يقوم فيها العميل بإرسال محاولات مُصادقة مع المُخدِّم المركزي خلال مدَّة زمنيَّة أقصاها 30 ثانية من بدأ تشغيله بعدها ينتقل إلى حالة النَّبضة.



2. **تهيئة الاتِّصال** : بعد أن يتعرَّف العميل على أنَّ المُخدِّم المركزي موجود، وجاهز بالعمل يقوم بالآتي:
   a. يُرسل مفتاح التَّشفير المُشفَّر الموجود لديه إلى المُخدِّم.
   b. يستلم المُخدِّم مفتاح التَّشفير، ويقوم بإلغاء ترميزه ثُمَّ إلغاء تشفيره.
   c. في حال كان المفتاح صحيحاً يقوم المُخدِّم بإرسال رسالة (Key Exchange Succeeded) إلى العميل لفتح قناة الاتِّصال، وغير ذلك يُنهى الاتِّصال تماماً.



3. **ارسال الأوامر بين ال server و ال client :**

من جهة السيرفر :

- يُرسل المخدِّم الأوامر باستخدام مفتاح تشفير خاص بالتواصل الإداري وتكون مشفرة باستخدام مفتاح مشترك موجود عن كلا الطرفين .

- الاستجابة من العميل تتضمن بينات الاستجابة الخاصة بالأمر الذي ارسله ال server مع معرّف فريد ID لتتبع الجلسة وتكون هذه الاستجابة مشفرة أيضا .

- يرسل المخدم رسالة تأكيد تتضمن المعرّف الفريد ID وفي حال عدم استلام المخدم للاستجابة خلال 30 ثانية يرسل المخدم رسالة تحقق من الاتصال (عن نجح الاتصال يعيد ارسال الأمر) و (إن لم ينجح يعيد المحاولة 5 مرات وبعدها يتم فصل الاتصال عند عدم الحصول على رد) .

- ينتظر المخدِّم رسالة تهيئة جديدة من العميل (ناتجة من حالة النبضة لدى العميل)

من هجة العميل :

1. استلام الأوامر:
   - يستلم الأمر بشكل ثنائي مشفّر.
   - يقوم بفك التشفير.
   - ينفذ الأمر المرسل.
2. إرسال الاستجابة:
   - يُرسل الاستجابة إلى المخدِّم بشكل ثنائي مشفّر.
   - يُرفق معها معرّف فريد.
3. في حال عدم استلام تأكيد الاستجابة خلال 30 ثانية:
   - يُرسل العميل رسالة تحقق من الاتصال
   - إن نجحت :يُعيد إرسال الاستجابة.
   - إن فشلت لأكثر من 5محاولات:
     - يدخل العميل في حالة النبضة

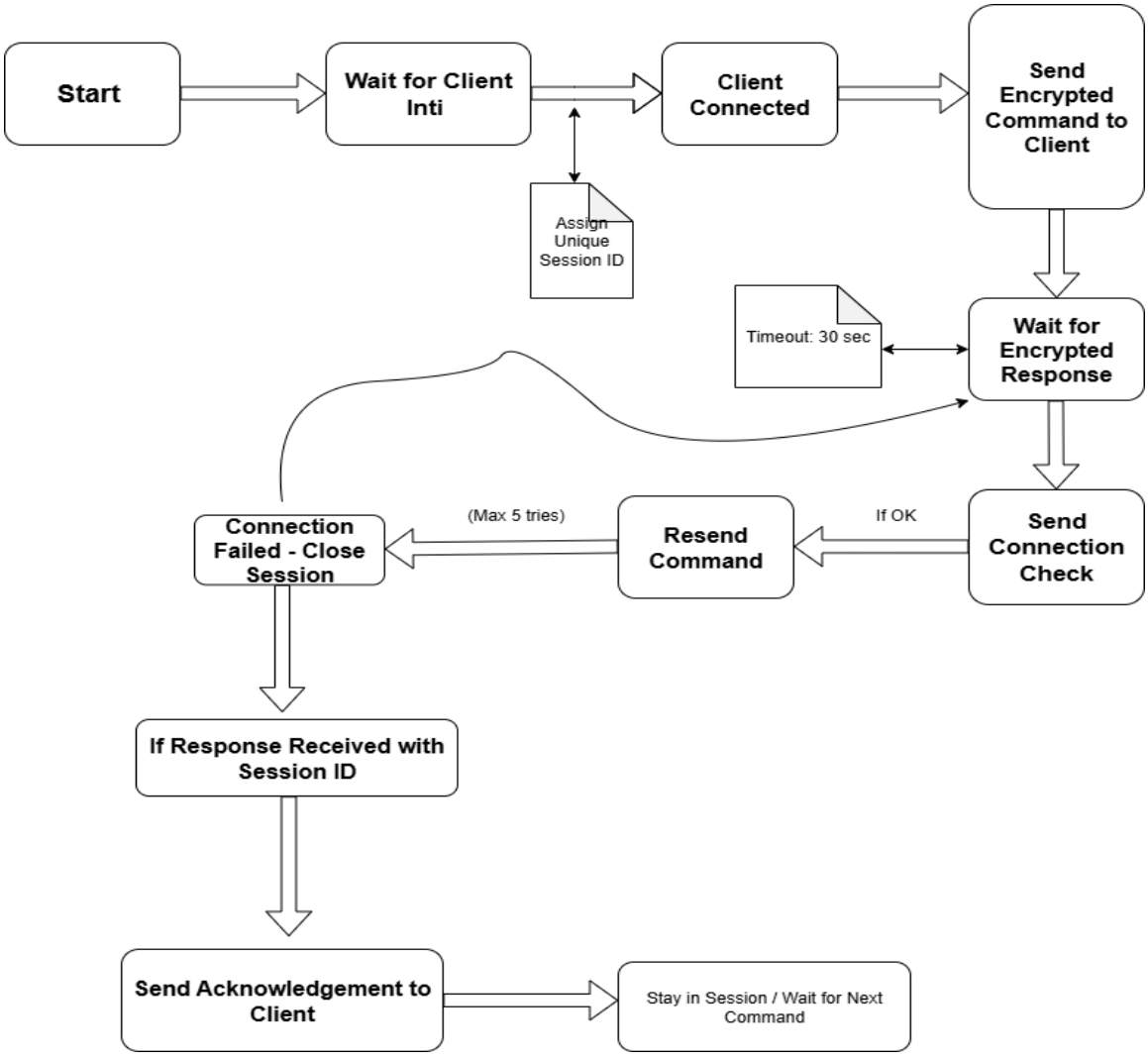
ملاحظة : عند تمام عملية تهيئة الاتصال من قبل الطرفين السيرفر يصنع thread ويقوم بتخزين العميل على شكل جلسة مع الاسم ورقم ال IPو ال port المناسبين ويتم التبديل بين الجلسات على أساس ال ID الخاص بكل جلسة .

4. حالة النَّبضة: هي حالة يدخل بها العميل في حال لم يقدر على الحصول على اتِّصال دائم مع المُخدِّم أو في حال انقطاع الاتِّصال تماماً مع المُخدِّم، وهي تُمثِّل حالة خمول تتألَّف من:
   a. يُرسل العميل رسالة استجابة للمُخدِّم أو يتحقَّق من الاتِّصال أو يحاول تهيئة الاتِّصال.
   b. لا ينجح أي من هذه العمليَّات في الحصول على الاستجابة المطلوبة من المُخدّم.
   c. بعد مرور 30 ثانية على المحاولات يدخل العميل في حالة النَّبضة حيث:
      i. يتوقَّف عن إرسال الرَّسائل إلى المُخدِّم.

ii. يوقف جميع الإجرائيَّات الَّتي تعمل تحت إشرافه.
iii. يقوم بإرسال رسالة نبضة كل دقيقتين إلى المُخدِّم.

d. في حال فشل الحصول على استجابة النَّبضة، لا يحدث شيء، ويستمر العميل بتأخير إرسال النَّبضة 10 ثواني مع كل رسالة إلى أن يصل لأقصى حد خمسة دقائق. أمَّا في حال حصل العميل على استجابة ناجحة للنَّبضة:
i. يُعيد تهيئة الاتِّصال مع المُخدِّم.
ii. يستأنف عمل جميع الإجرائيَّات الَّتي تعمل تحن إشرافه.

من جهة ال server



من جهة ال Client