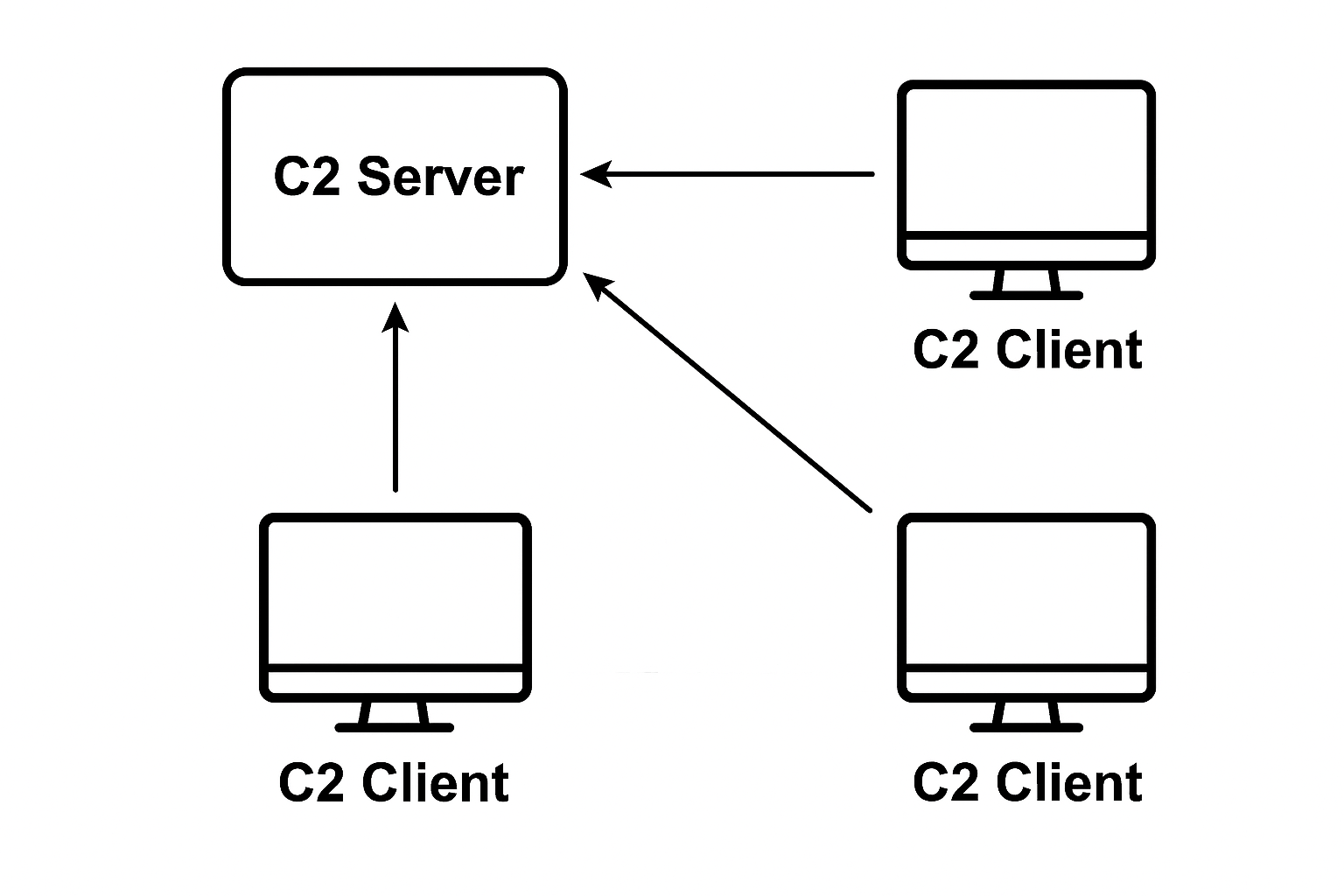
# C2 Reverse Shell

قبل الحديث عن العنوان بشكل أكاديمي سوف نأخذ مثال من الحياة العملية لنتخيل أن مدير شركة جالس بمكتبه يملك ملفات لمجموعة من الموظفين و يعطي الأوامر للموظفين الموجودين في فروع بعيدة خارج الشركة ويتواصلون بالهاتف ويأخذون الأوامر ويمكن للمدير أن يفتح الملف الخاص بكل موظف ويعطي الأوامر ويستطيع إعطاء أوامر مختلفة لكل موظف في نفس الوقت وبشكل مستقل ...و بالإسقاط على الحياة الأمنية تخيل مجموعة في البنك اخترقت حاسوب في بنك و حاسوب في مطار و حاسوب في شركة اتصالات هنا كل حاسوب يشغل c2 client يتصل هذا العميل بسيرفرهم السري و الهاكرز يدخل إلى الوحة التحكم و يرى 3 أجهزة متصلة ويرسل الأمر للجهاز الأول لسرقة كلمة السر و أمر للثاني للتجسس و أمر للثالث بحذف أو تشفير الملفات مثلا .

**بالمختصر:**  
الهاكرز يتحكم عن بعد بعدة أجهزة مصابة بسهولة وكأنهم موظفين ينفذون أوامر عبر خط اتصال خفي.



**الية عمل نظام C2 بالتفصيل :**

* **الخادم C2 Server :** ينتظر الاتصالات الواردة من الأجهزة المصابة . Clients
* **العميل C2 Client :** يكون كود خفي يعمل على جهز الضحية يرسل الاتصال إلى الخادم .

الخادم يقوم بإعطاء الأوامر للعملاء مثل رفع أو تنزيل او حذف ملفات والعميل ينفذ الأوامر و يُظهر النتائج ويمكن تشفير الاتصال لمنع اكتشافه من قبل جدران الحماية .

**مواصفات الخادم :**

* متعدد جلسات Multi Threading : عندما يتصل عميل جديد تَظهر جلسة خاصة به new session و يضع الجلسة في قائمة الجلسات المفتوحة .
* حرية الاختيار : يمكن للخادم اختيار أي جلسة و التحكم بها من دون التأثير على الجلسات الأخرى .

Client 1 (جهاز مصاب 1) - > يتصل - > Session 1

Client 2 (جهاز مصاب 2) - > يتصل - > Session 2

Client 3 (جهاز مصاب 3) -> يتصل - > Session 3

**الية برمجة C2 Server و C2 Client نظريا :**

**برمجة العميل :**

* إنشاء اتصال بالخادم.
* إرسال بعض المعلومات مثل اسم الجهاز ، IP، نظام التشغيل
* انتظار الأوامر.
* تنفيذ الأوامر.
* إعادة إرسال النتائج.

**Open connection with server** - > **send ID** - > **wait command** -> **execute command** - > **send result**

**برمجة الخادم :**

السيرفر يستمع على بورت معين (مثلاً: 8080).

عند وصول اتصال:

* يقبل الاتصال.
* ينشئ Thread (خيط تنفيذ مستقل) لكل عميل.
* يحفظ معلومات كل جلسة.

يسمح لك:

* باستعراض جميع الأجهزة المتصلة.
* اختيار جهاز معين.
* إرسال أوامر له واستقبال النتائج.

