الجمهورية العربية السورية

وزارة التعليم العالي

جامعة اللَّاذقية

كلية الهندسة المعلوماتية

قسم النُّظم والشَّبكات الحاسوبية

مشروع نظم رقميَّة مُبرمجة

C2 Server/Client

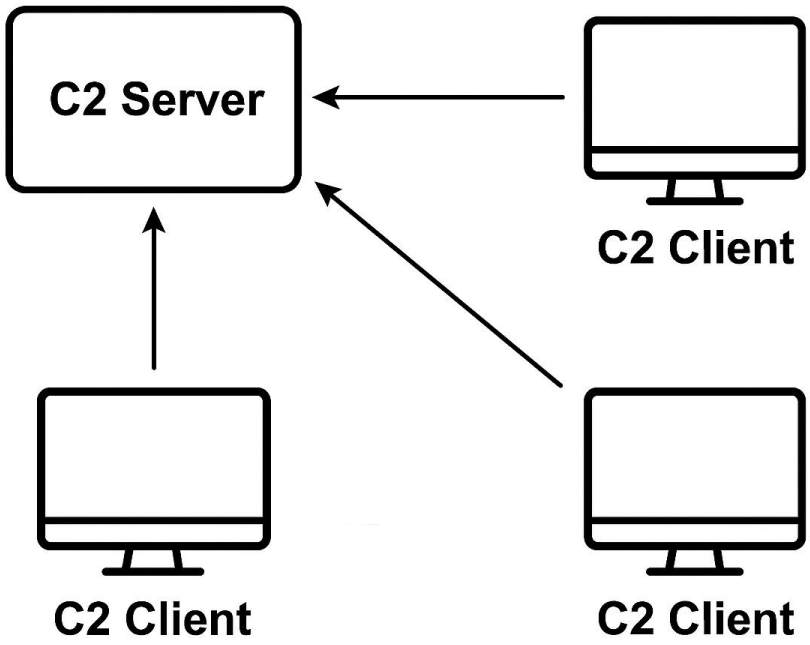
إعداد:

محمد مؤذِّن – يزن محسن الجَّداوي – حسين شنن

2025م

يُستخدم مُصطلح (Command and Control Server) إلى المُخدِّم الَّذي يقوم أعضاء الفريق الهجومي في الأمن السِّيبراني باستخدامه بشكل أساسي من أجل الحفاظ على اتِّصال مُستقر، ودائم مع جميع الأجهزة الَّتي تمَّ الوصول، وذلك من أجل تحقيق وصول مركزيٍّ لكل أجهزة الهدف لتسهيل التَّعامل معها بواسطة كُلِّ أعضاء الفريق الهجومي بشكل سلس، ولا يقتصر دور ال (C2 Server) على اعتباره نقطة اتِّصال مركزيَّة فحسب، بل يُستخدم أيضاً في توفير العديد من الميِّزات، والخصائص الَّتي تدعم عمليَّات الأمن السِّيبراني الهجومي وهي تتمثَّل، ولا تنحصر في:

- الرَّفع، والتَّنزيل.
- التقاط صورة شاشة لجهاز الهدف.
- تحقيق اتِّصال مُتزامن مع العديد من الأهداف في نفس الوقت.
- تحقيق اتِّصال خامل يعتمد على مبدأ ال (Heartbeat).
- تحقيق اتِّصال آمن مُشفَّر بين المُهاجم، والهدف.
- تنفيذ إجرائيَّات، ومهام أمنيَّة عن طريق الاعتماد على ال (Native API) للهدف بدلاً من الأوامر التَّقليديَّة سهلة الكشف.
- تطبيق العديد من التِّقنيات الأمنية المُعقَّدة أو تحميل أدوات تُستخدم في العمليَّات السِّيبرانيَّة الهجومية.



آلية عمل (C2 Server/Client) بالتفصيل:

- C2 Server: ينتظر الاتصالات الواردة من الأجهزة الهدف كما يُعتبر المسؤول عن عمليَّة تنظيم الاتصالات بينه، وبين جميع الأهداف.
- Client: هو تطبيق برمجي يُنفَّذ على جهاز الهدف، ويعمل على تنفيذ جميع الأوامر الصَّادرة من المُخدِّم حيث ينُفِّذ العملية ثُمَّ يُعيد النَّتيجة.

باختصار الخادم يعطي الأوامر للعملاء مثل رفع أو تنزيل او حذف ملفات والعميل ينفذ الأوامر، ويرسل النَّتيجة.

تحقيق التَّزامن:

هناك طريقتان يُحقَّق بهما التَّزامن في المشروع:

1- تزامن الاتِّصال: وذلك عن طريق اتِّصال عدِّة عُملاء بالمُخدِّم في وقتٍ واحد.

2- تزامن الإجرائيَّات:

a. تزامن الإجرائيَّات في المُخدِّم: وذلك عن طريق الإشراف على تنفيذ العديد من الإجرائيَّات الخاصَّة بمُختلف العُملاء.

b. تزامن الإجرائيَّات في العميل: يُحقَّق ذلك عن طريق السَّماح للعميل نفسه بإنشاء إجرائيَّات جديدة، والتَّحكم بها، وإنهائها حسب الحاجة.

أدوات التَّطوير:

هُناك قسمان للمشروع:

1- المُخدِّم: وسيُطوَّر باستخدام لغة البرمجة (Python).

2- العميل: سيطوَّر باستخدام لغة البرمجة (Rust)، وذلك لضرورة الحصول على نسخة نهائية (Compiled) للعميل لكي يعمل على جهاز الهدف دون الحاجة لأي برمجيَّات أُخرى.