يرسلـه المتجسس إلى جهاز الضحية فيقوم الأخير بحسن نية بتشغيل هذا الملف ظنا منه بأنه برنامج مفيد لكنه غالبا ما يفاجأ بعدم عمل الملف بعد النقر عليه فيظن انه ملف معطوب.. فيبحث عن شيء آخر أو برنامج ثاني ويهمل الموضوع بينما في ذلك الوقت يكون المتجسس قد وضع قدمه الأولى داخل جهـاز الضحـيـة،، ويتم الاتصال بين الجهازين عبر منفذ اتصال لكل جهاز ، قد يعتقد البعض ان هذا المنفـذ مـادي باسـتطاعته ان يراه أو يلمسه مثل منفذ الطابعة أو المأوس ، ولكنه جزء من الذاكرة له عنوان معين يتعرف عليـه الجهـاز بأنـه منطقة يتم إرسال واستقبال البيانات عليها ويمكن استخدام عـدد كبيـر مـن المنافـذ للاتصـال وعـددها يقـارب ٦٥٠٠٠ منفذ تقريبا ، يميز كل منفذ الآخر رقمه فمثلا المنفذ رقم ٨٠٨٠ يمكن إجراء اتصال عن طريقـة ، وفـي نفس اللحظة يتم استخدام المنفذ رقم ٨٠٠٠ لإجـــراء اتصـــــــال أخـــــــــر

وعند الإصابة ببرنامج الخادم فانه يقوم في أغلب الأحـوال بما يلي :

١- الاتجاه إلى ملف تسجيل النظام (registry) حيـث ان النظـام فـي كـل مـرة تقـوم بتشـغيل الوينـدوز يقـوم بتشغيل البرامج المساعدة في ملف تسجيل النظام مثل برامج الفيروسات وغيرها.
٢- يقوم بفتح ملف اتصال داخل الجهاز المصاب تمكن برنامج العميل من النفوذ
٣- يقوم بعملية التجسس وذلك بتسجيل كل ما يحدث أو عمل أشياء أخرى على حسب ما يطلـب منـه هـذا يعني ان الجهاز إذا أصيب فانه يصبح مهيأ للاختراق، وبرنامج الخـادم ينتظـر طلـب اتصـال فـي أي لحظـة عـن طريق المنفذ الذي قام بفتحه ، ويأتي طلب الاتصال بأحد طريقين :

ا- من قبل شخص يتعمد اختراق الجهاز المصاب بعينة، وذلك لعلمه بوجود معلومات تهمه أو لإصابة ذلك الجهاز بالضرر لأي سبب كان
ب- من قبل شخص لا يتعمد اختراق هذا الجهاز بعينة، ولكنه يقوم بعمل مسح scanning على مجموعة مـن الأجهزة في نطاق معين من العناوين لمعرفة أيها الذي لديه منافذ مفتوحة وبالتالي فهو قابـل للاختراق.

ما هو رقم الآي بي أدرس (IP(Internet protocol:

==========

تنتمي لعائلة TCP/IP وهو عبارة عن بروتوكول يسمى IP اختصار Internet Protocol
فلكي يتواجد شخص معين على شبكة الانترنت لابد ان تكون له هوية تمثله وهـذه الهويـه هـي الاي بـي و تكون من أربع أرقام وكل مستخدم على الشبكة له رقم لا يمكن لآخر ان يدخل به في نفس الوقت
مثل السيارة التي في الطريق كل سيارة لها الرقم الخاص بها و مستحيل يكون في سيارة لها نفس الـرقم و يتكون من أربع مقاطع كل مقطع يكون من ٠ -----> ٢٥٥
و العنونة على الشبكة تتم عن طريق تقسيم العناوين إلى أربعة نطاقات
(A) (B) (C) (D)
١- فالمستخدم العادي يستخدم أي بي من نطاق D و اقصد عنوان على شكل مثال "١٦٣,٢,٦,٤"
وذلك يعني ان الأربعة مقاطع محدده و ثابتة لا تتغير .

٢- اما الشركات تمتلك اي بي من نطاق C فهي تمتلك عنوان على هيئة ١٩٣,٢٥٥,٣,***
و مالك هذا العنوان يستطيع إعطاء إي قيمة تتراوح بين ٢٥٥ ----> ٠ اي انه يعطي ٢٥٥ رقم مثل : -
١٩٣,٢٥٥,٣,١
١٩٣,٢٥٥,٣,٢
١٩٣,٢٥٥,٣,٣
.
.
.
١٩٣,٢٥٥,٣,٢٥٥

٣- نطاق B ويكون على شكل ١٩٣,٢٢٥***.***
و يستطيع صاحبه إعطاء أرقام مثل : -
١٩٣,٢٢٥'١'١
١٩٣,٢٢٥'١'٢
١٩٣,٢٢٥'١'٣
.
.
.

١٩٣,٢٢٥'٣'١

ياسر رجب التهامي- جمهورية مصر العربية
Y_tohamy@hotmail.com