



การโจมตีด้วยโทรจัน (Beast)

จัดทำโดย

1. นายณัฐพันธ์	กันเสนา	553020436-2
2. นางสาวนงนภา	ไต้หนองแปน	553020448-5
3. นางสาวรัตนา	มอบสันเทียะ	553020464-7
4. นางสาวอภิญา	ไสยโสภณ	553020476-0
5. นางสาวณัฐธิดา	โพธิ์สว่าง	553020984-1
6. นางสาวสุธีกานต์	แต่สกุล	553021030-5

นักศึกษาระดับปริญญาตรี ชั้นปีที่ 3

หลักสูตรวิทยาการคอมพิวเตอร์ สาขาวิชาเทคโนโลยีสารสนเทศและการสื่อสาร (ภาคพิเศษ)

เสนอ

ผศ.ดร.จักรชัย โสอินทร์

วิชา 322376 INFORMATION AND COMMUNICATION TECHNOLOGY SECURITY

Section 4

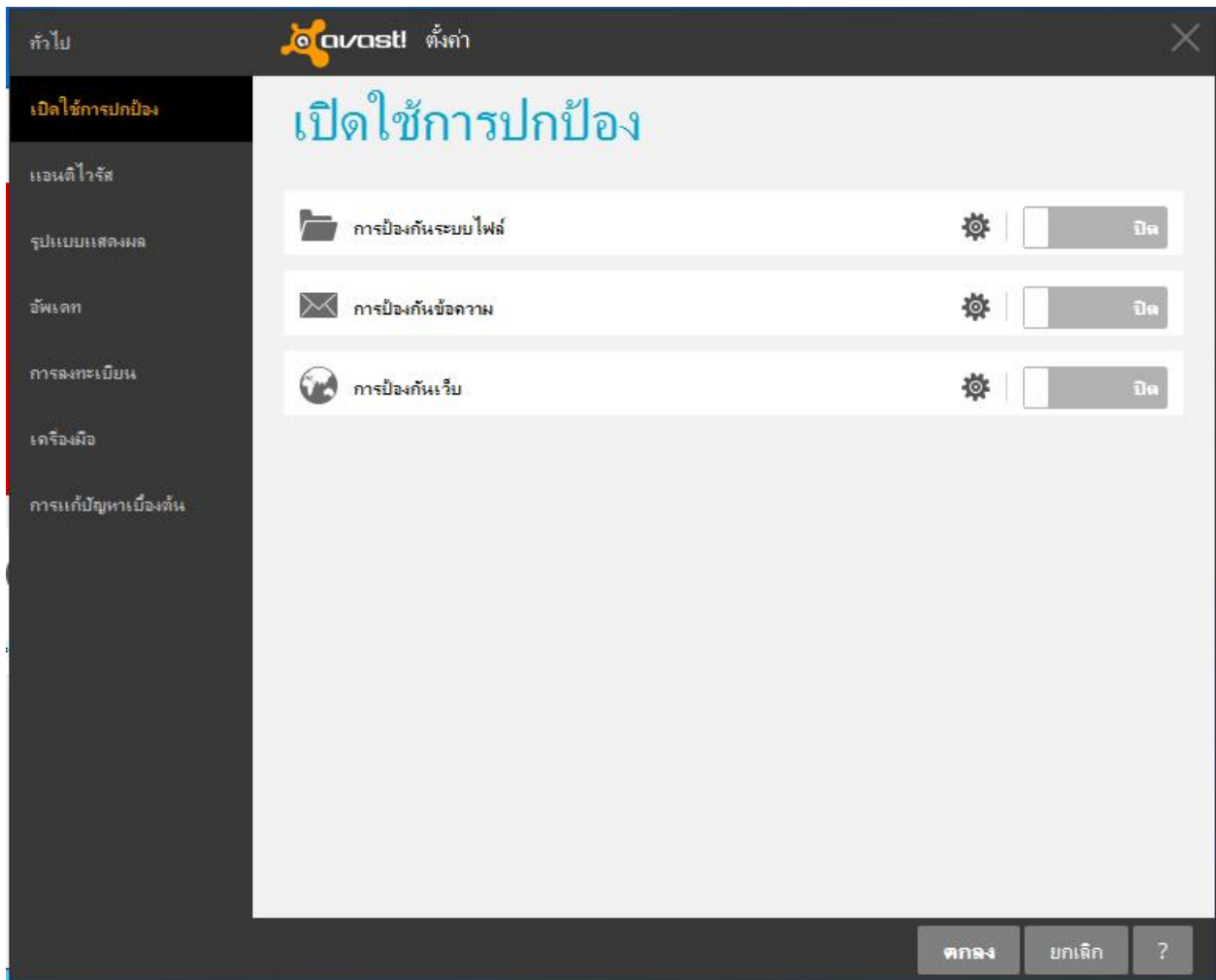
ภาคการศึกษาที่ 1 ปีการศึกษาที่ 2557

คณะวิทยาศาสตร์ มหาวิทยาลัยขอนแก่น

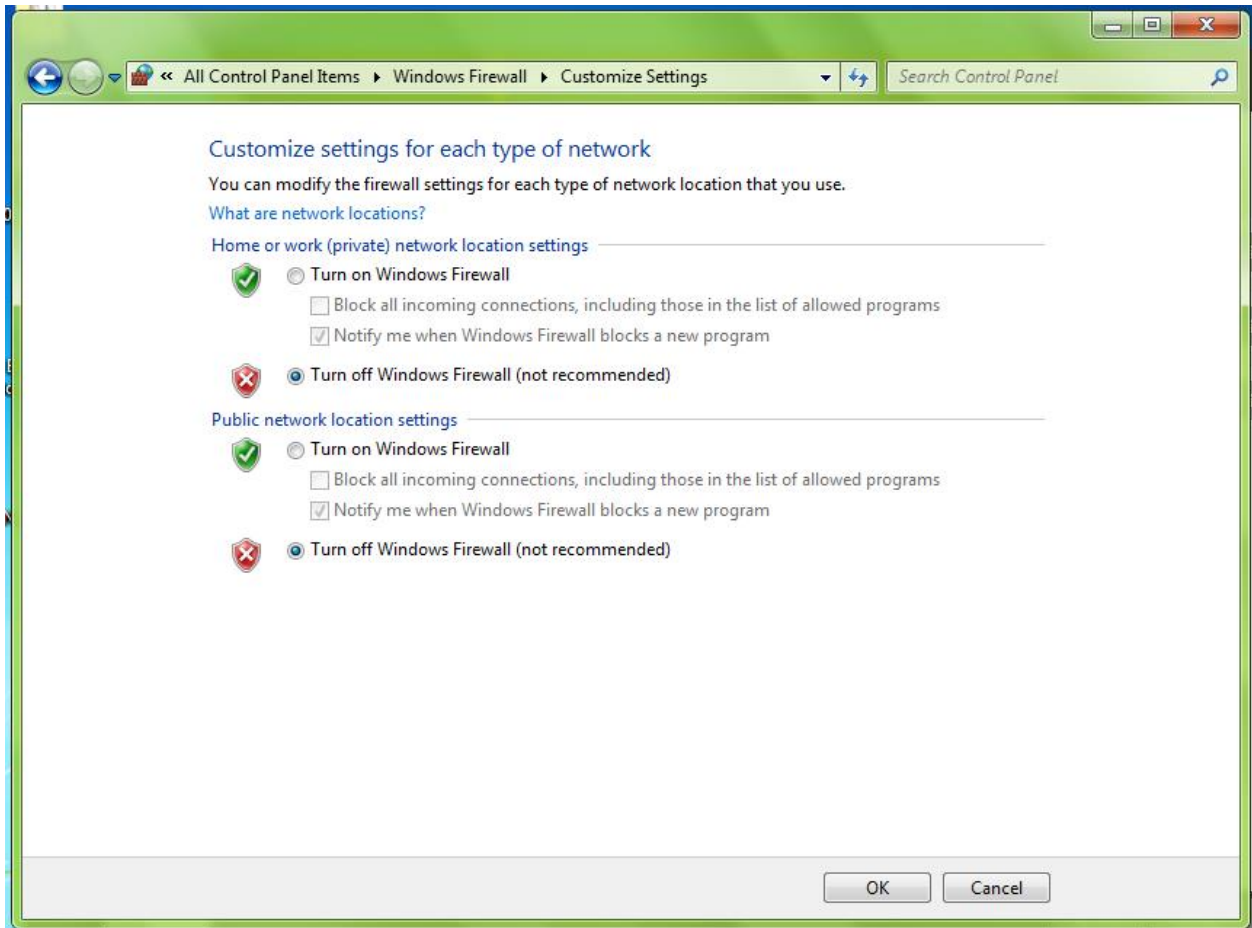
คำนำ

รายงานฉบับนี้เป็นส่วนหนึ่งของวิชา 322376 INFORMATION AND COMMUNICATION TECHNOLOGY SECURITY กลุ่ม 4 ของนักศึกษาชั้นปีที่ 3 สาขาเทคโนโลยีสารสนเทศและการสื่อสาร โดยมีจุดประสงค์เพื่อนำเสนอเนื้อหาเกี่ยวกับม้าโทรจัน ซึ่งรายงานนี้มีเนื้อหาความรู้เรื่องการโจมตี โดยการฝังม้าโทรจันไว้ที่เครื่องของฝ่ายตรงข้าม ผู้จัดทำได้เลือกหัวข้อนี้ในการทำรายงาน เนื่องจากเป็นเรื่องที่น่าสนใจ การจัดทำรายงานนำเสนอเนื้อหาข้อมูลในครั้งนี้ เพื่อเป็นแนวทางการศึกษา ผู้จัดทำหวังว่ารายงานฉบับนี้จะให้ความรู้ และเป็นประโยชน์แก่ผู้อ่านทุก ๆ ท่านหากมีข้อผิดพลาดประการใดต้องขออภัยมา ณ ที่นี้ด้วย

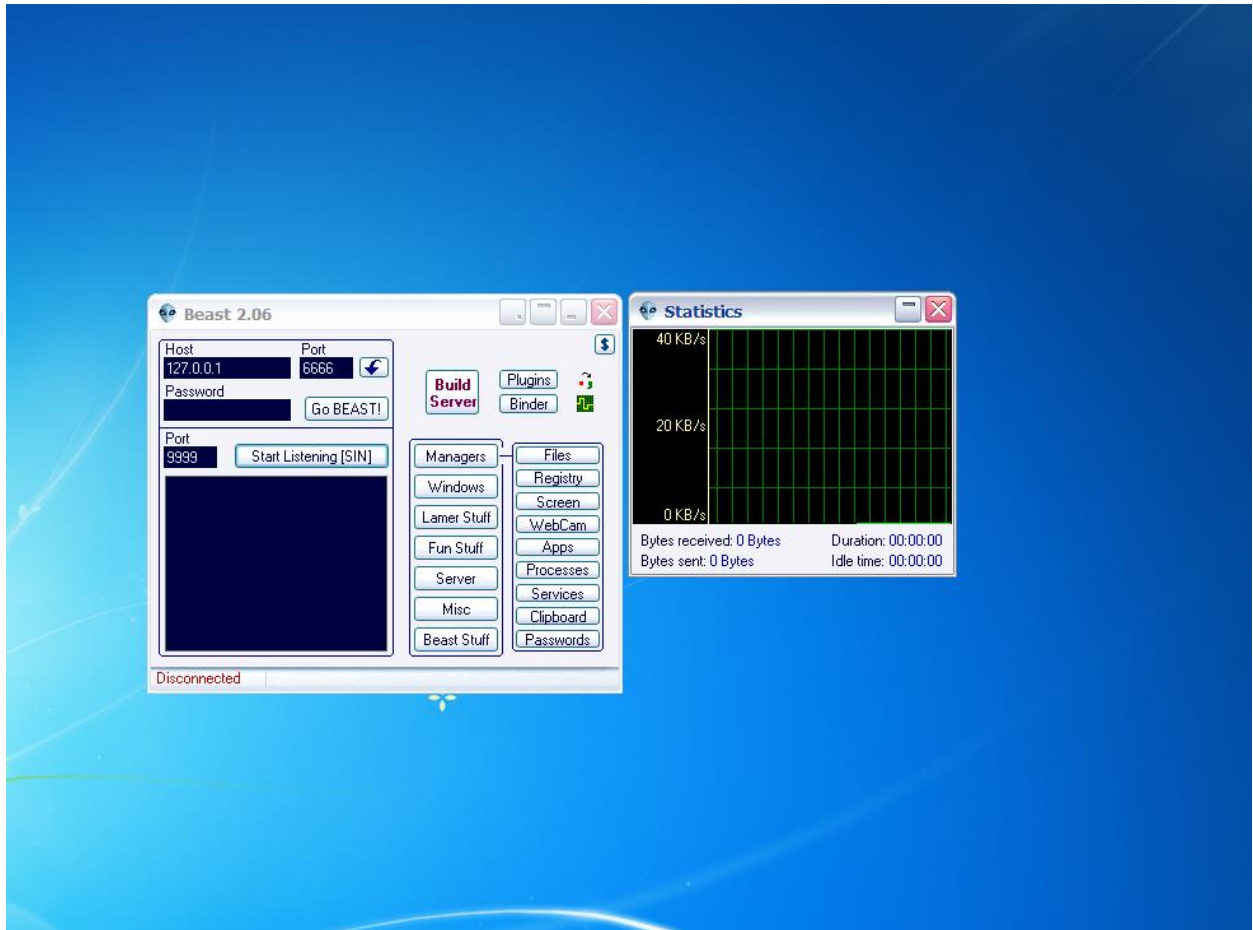
คณะผู้จัดทำ



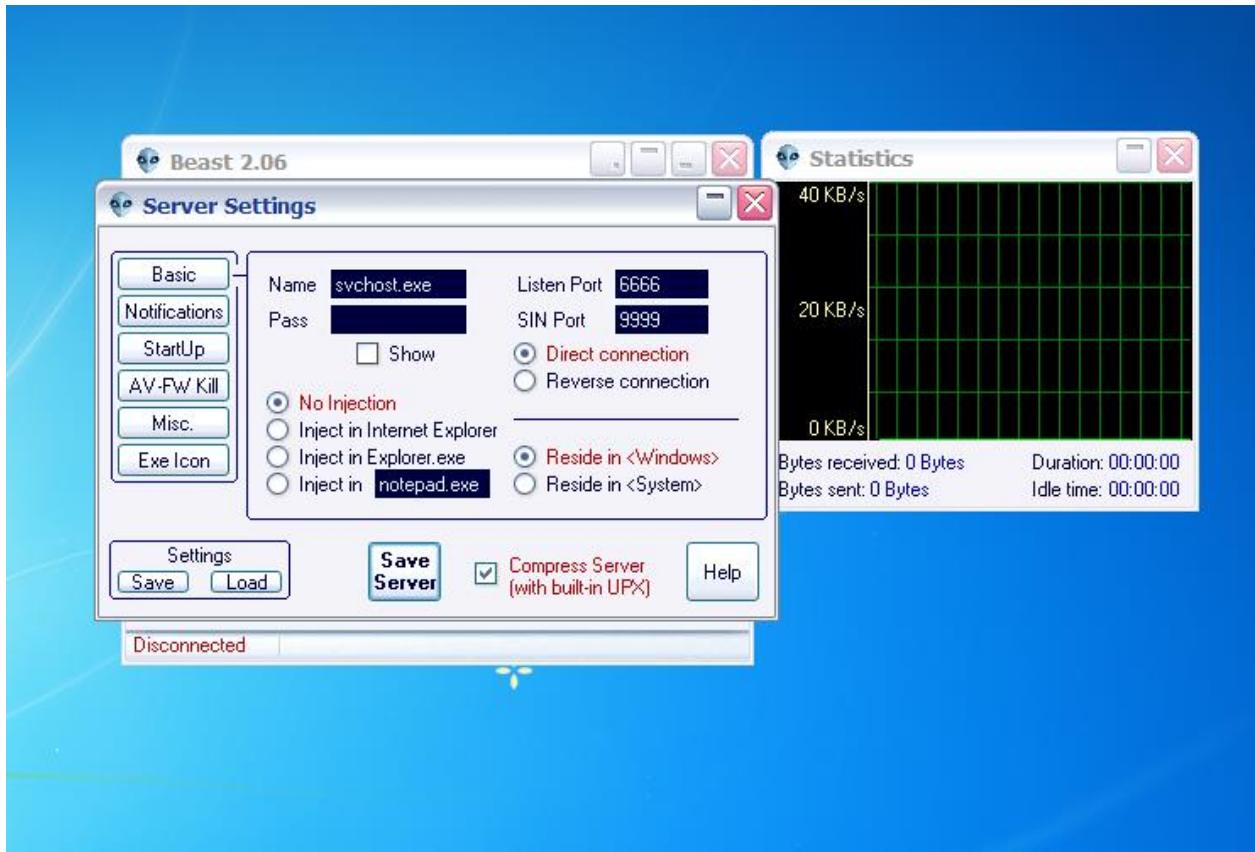
รูปที่ 1 : ปิดโปรแกรมสแกนไวรัสภายในเครื่อง



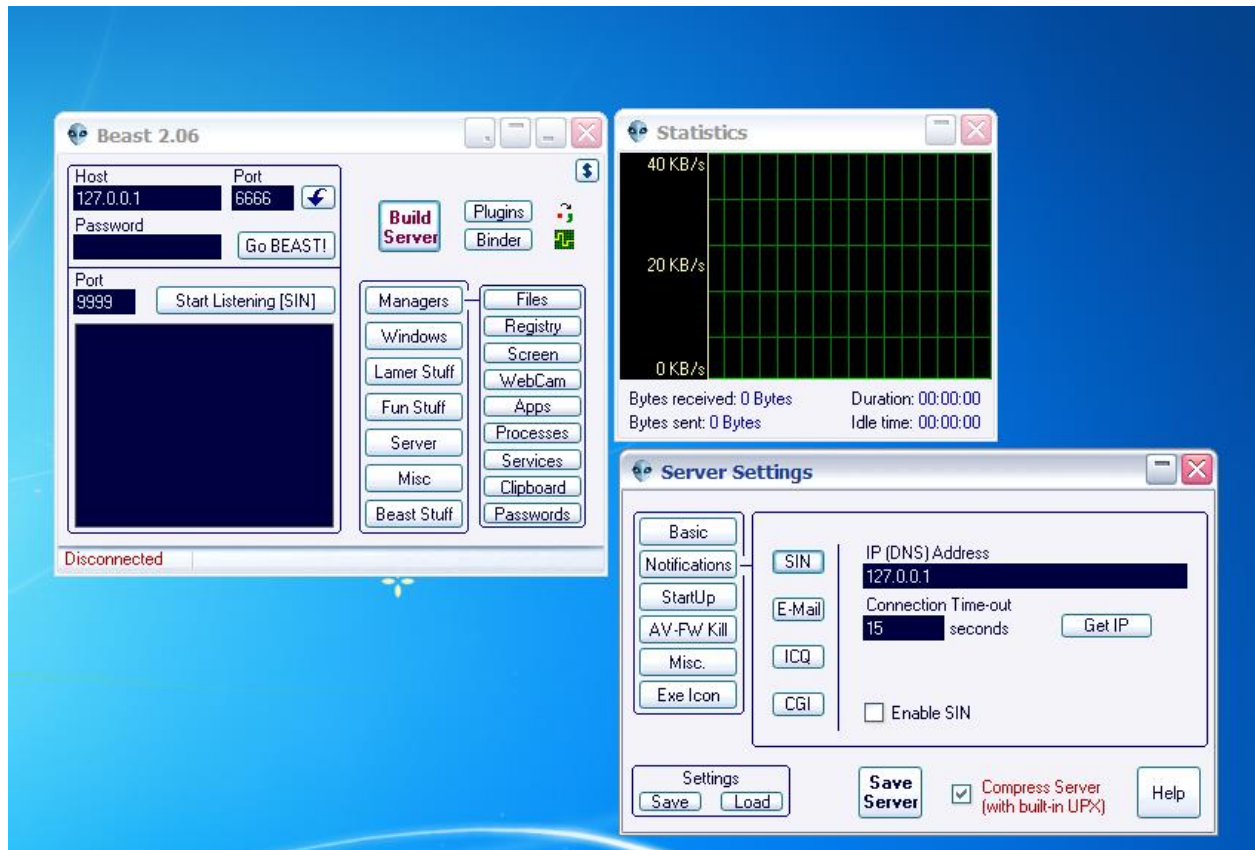
รูปที่ 2 : ปิด windows Firewall



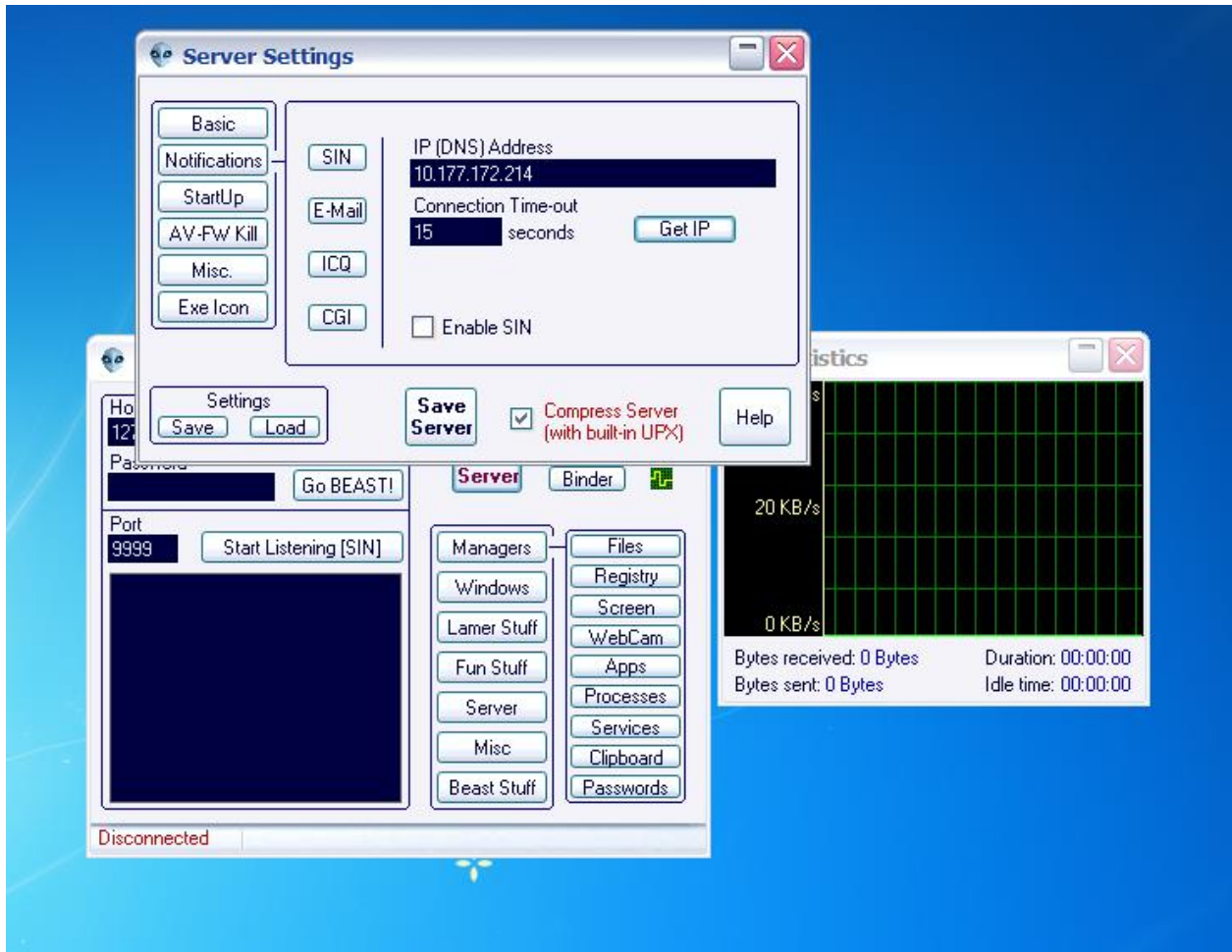
รูปที่ 3 : เข้าโปรแกรมแล้วกด **Build Server**



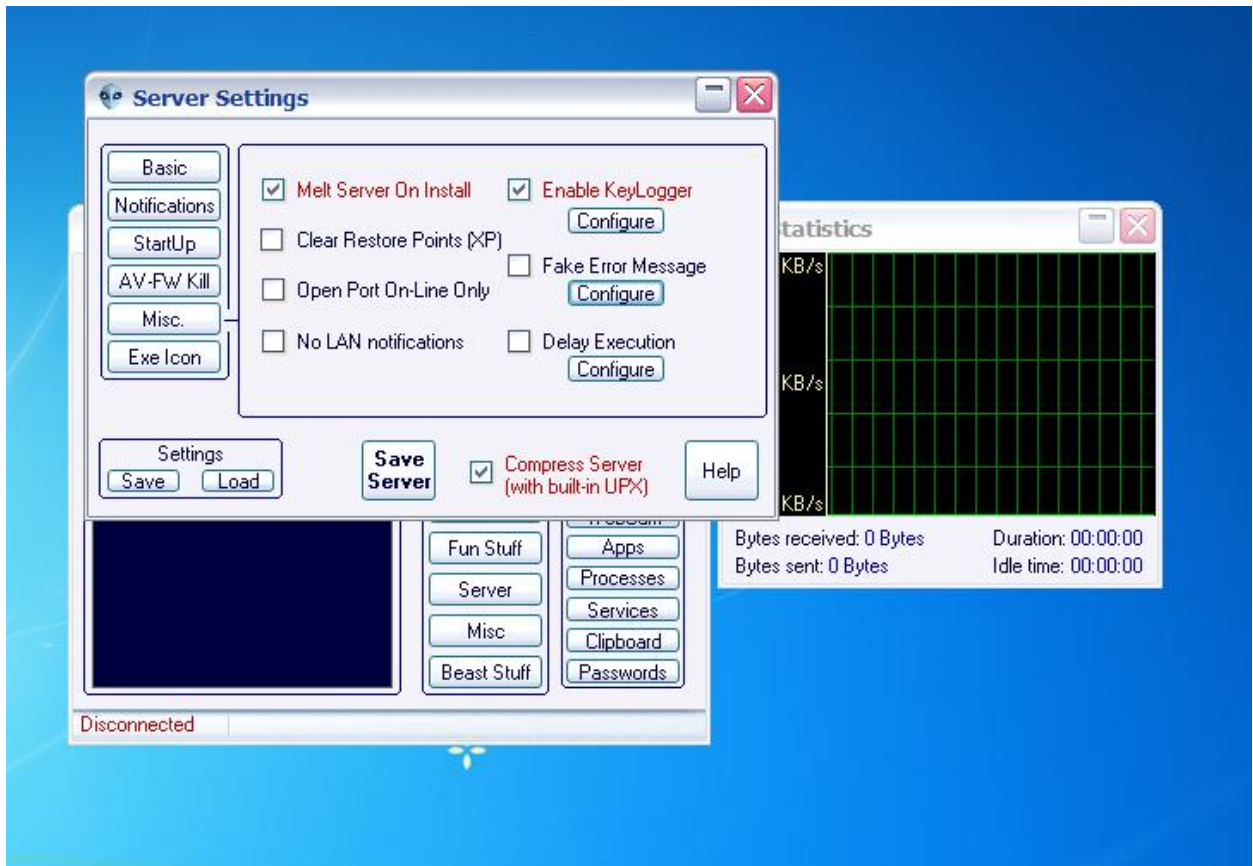
รูปที่ 4 : ในแท็บ Basic เปลี่ยนจาก Direct connection เป็น Reverse connection



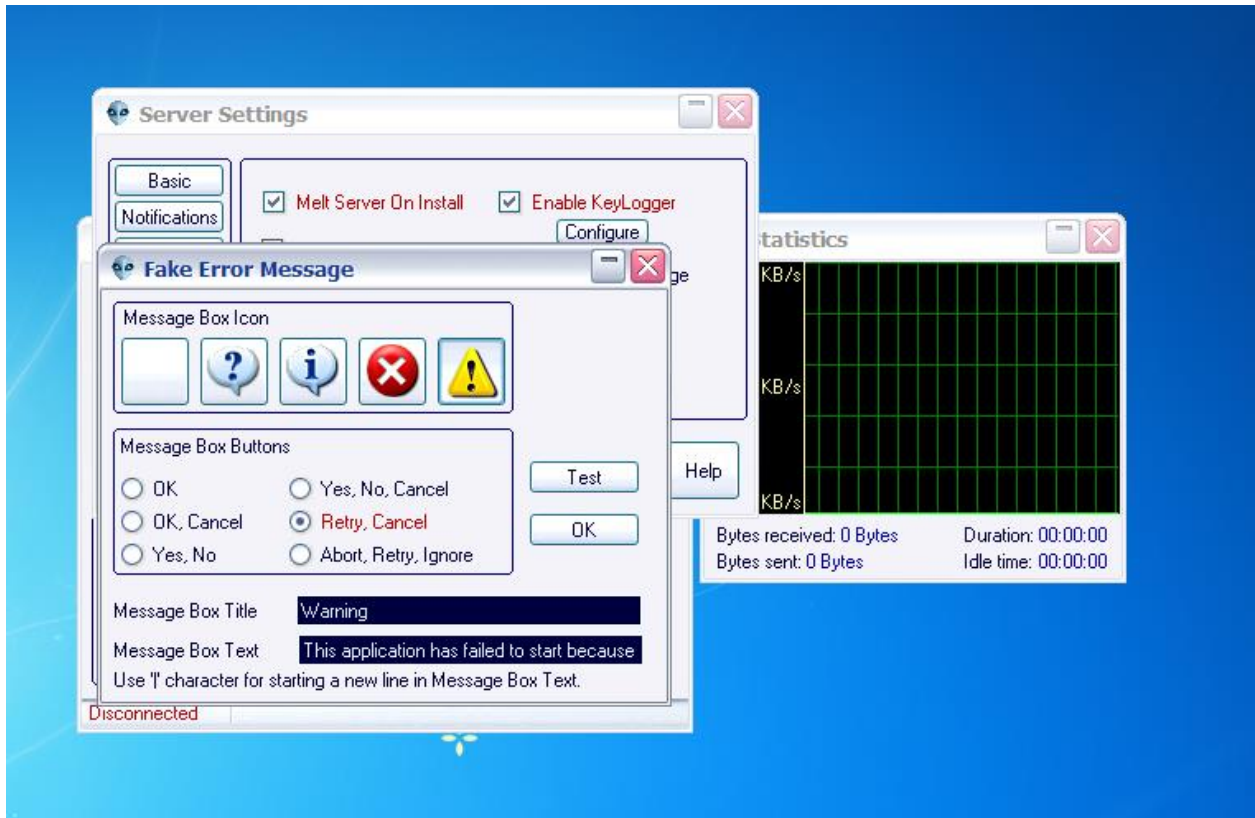
รูปที่ 5 : ในแท็บ Notification กดปุ่ม Get IP เพื่อใช้กำหนด IP Address ของเครื่องที่จะใช้โจมตี



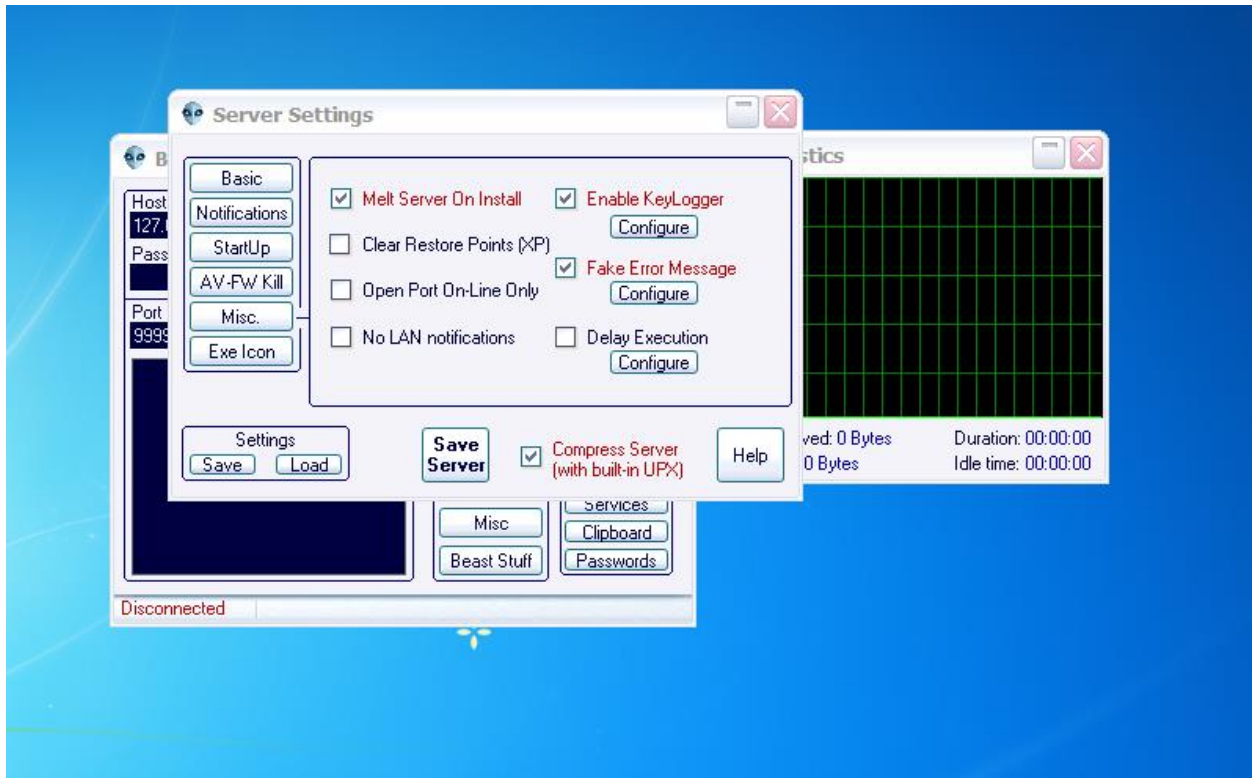
รูปที่ 6 : โปรแกรมจะแสดง IP ของเครื่องดังภาพ



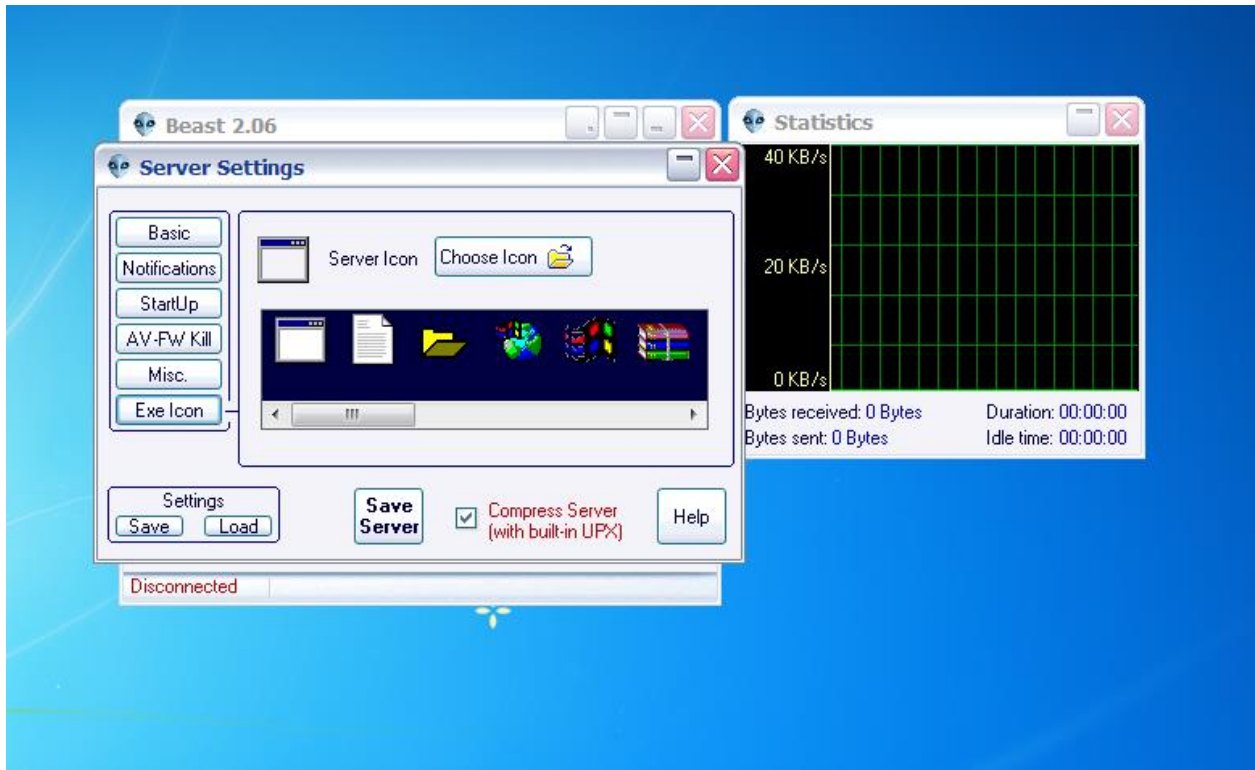
รูปที่ 7 : ในแท็บ Misc. กำหนดข้อความแสดงข้อผิดพลาดแจ้งเครื่องเป้าหมาย



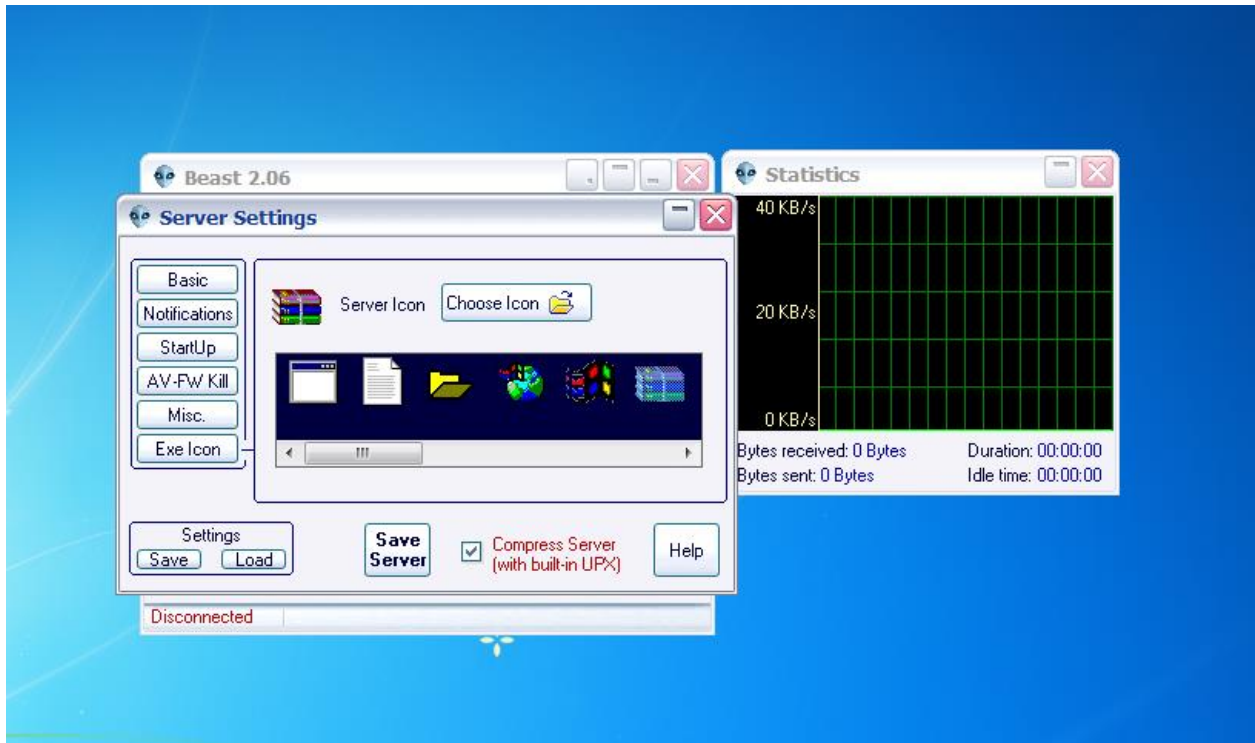
รูปที่ 8 : เลือกไอคอนและข้อความแสดงผลแล้วกด OK



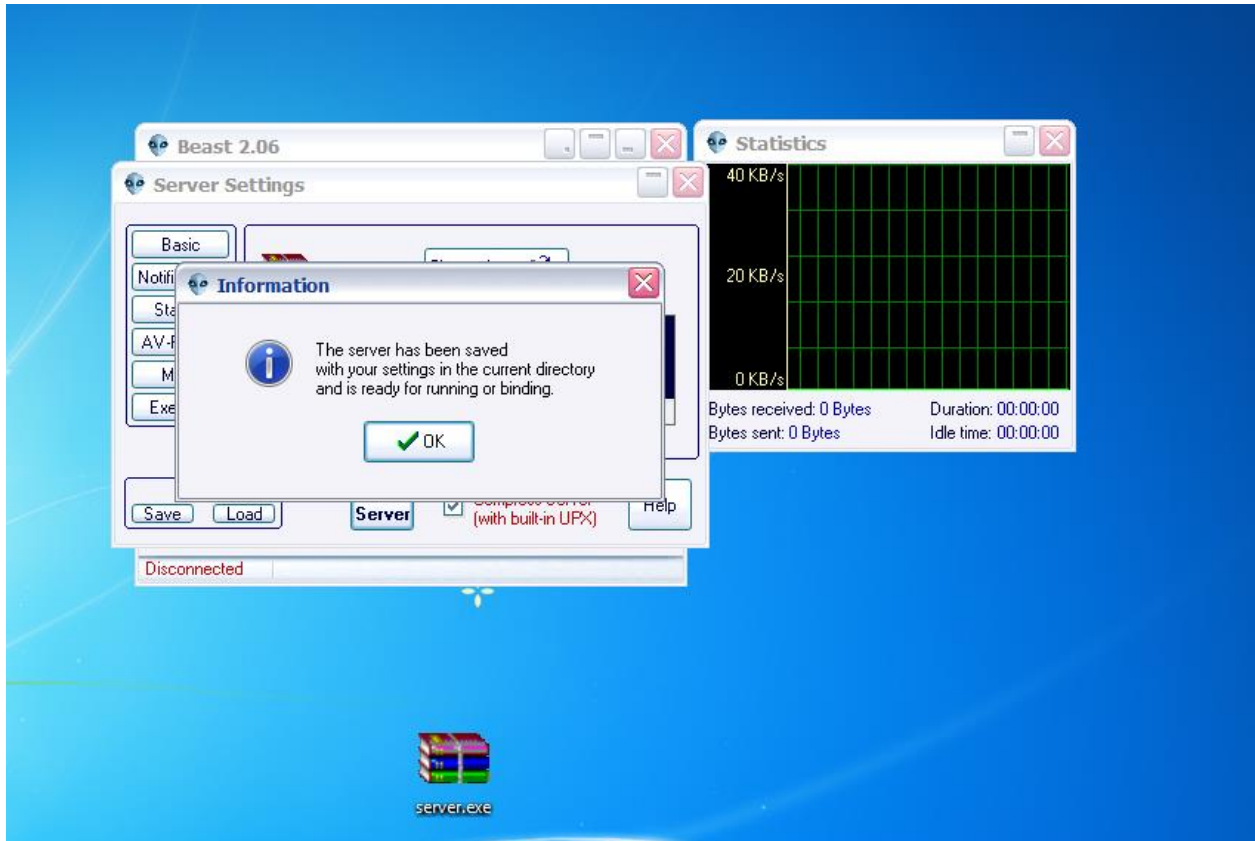
รูปที่ 9 : เลือกเครื่องหมายถูก Fake Error Message เพื่อเปิดใช้งานการตั้งค่า



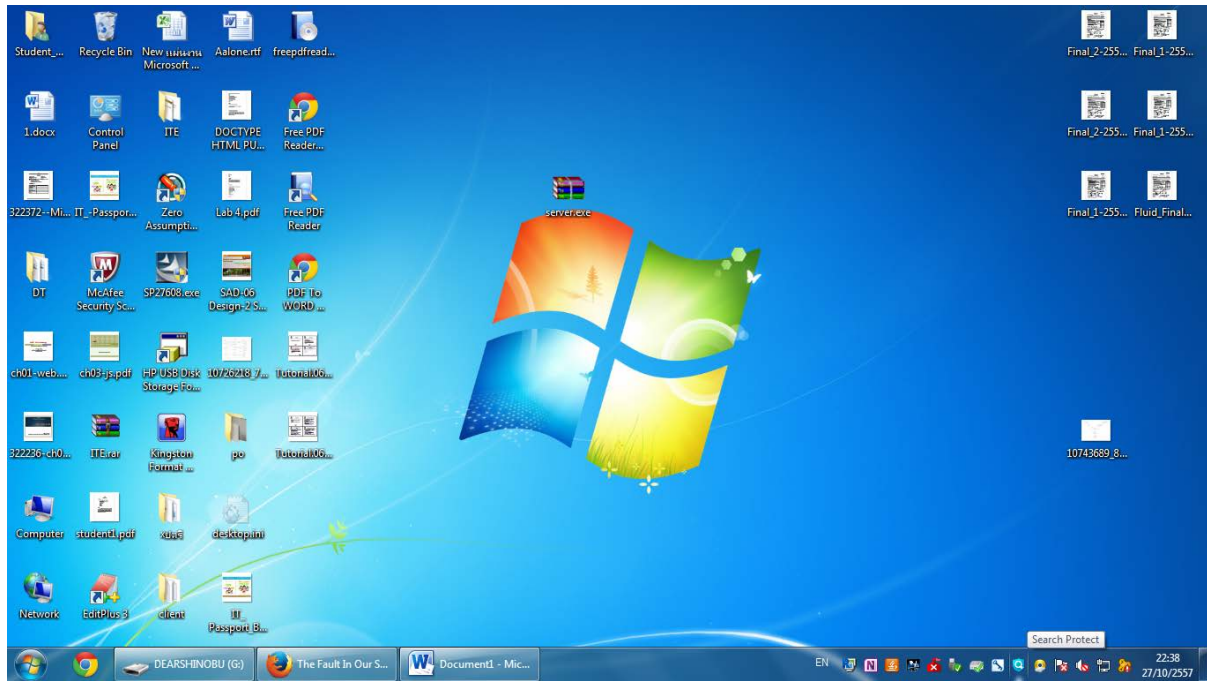
รูปที่ 10 : Exe Icon เลือกไอคอนที่จะนำไปวางในเครื่องเป้าหมาย



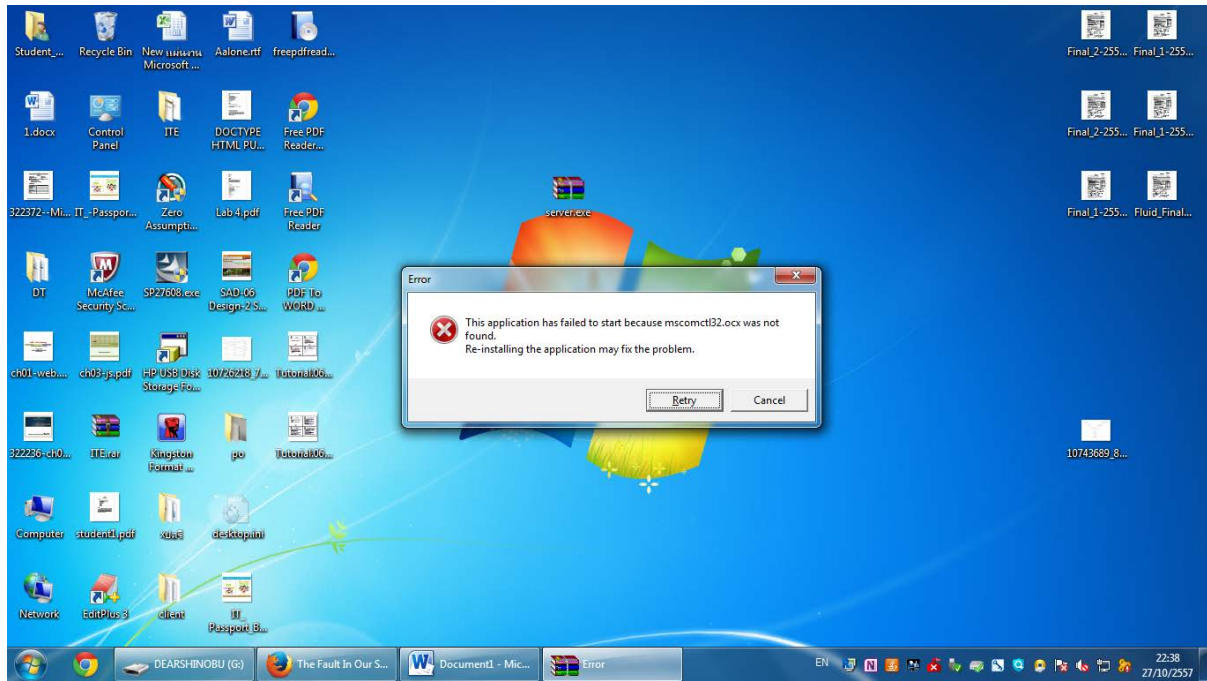
รูปที่ 11 : กดเลือก Save Server



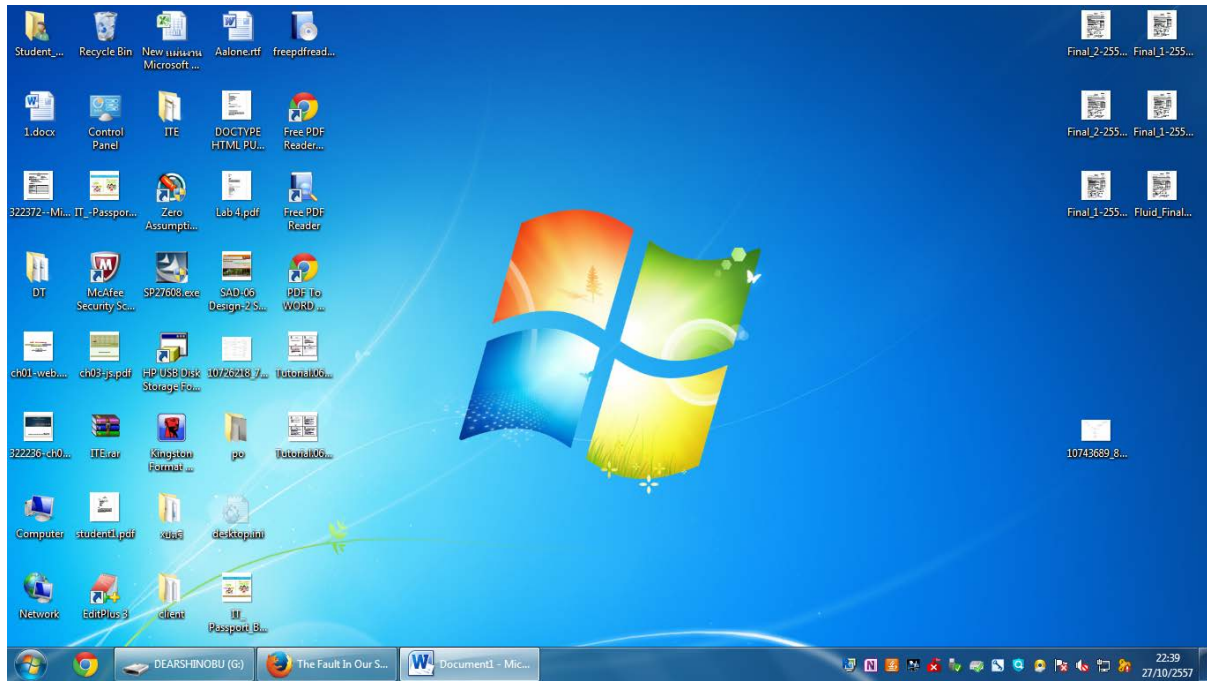
รูปที่ 12 : โปรแกรมแสดงข้อความแจ้งว่า ทำการสร้างไฟล์ .exe ไว้เรียบร้อยแล้ว



รูปที่ 13 : นำไฟล์ .exe ที่สร้างไว้ไปเปิดในเครื่องเป้าหมาย โดยที่เครื่องเป้าหมายต้องปิด Windows Firewall และโปรแกรมสแกนไวรัส



รูปที่ 14 : ดับเบิลคลิกที่ไฟล์ .exe จากนั้นระบบจะแจ้งเตือนข้อความ(ที่เครื่องไฮสตั้งค่าไว้)



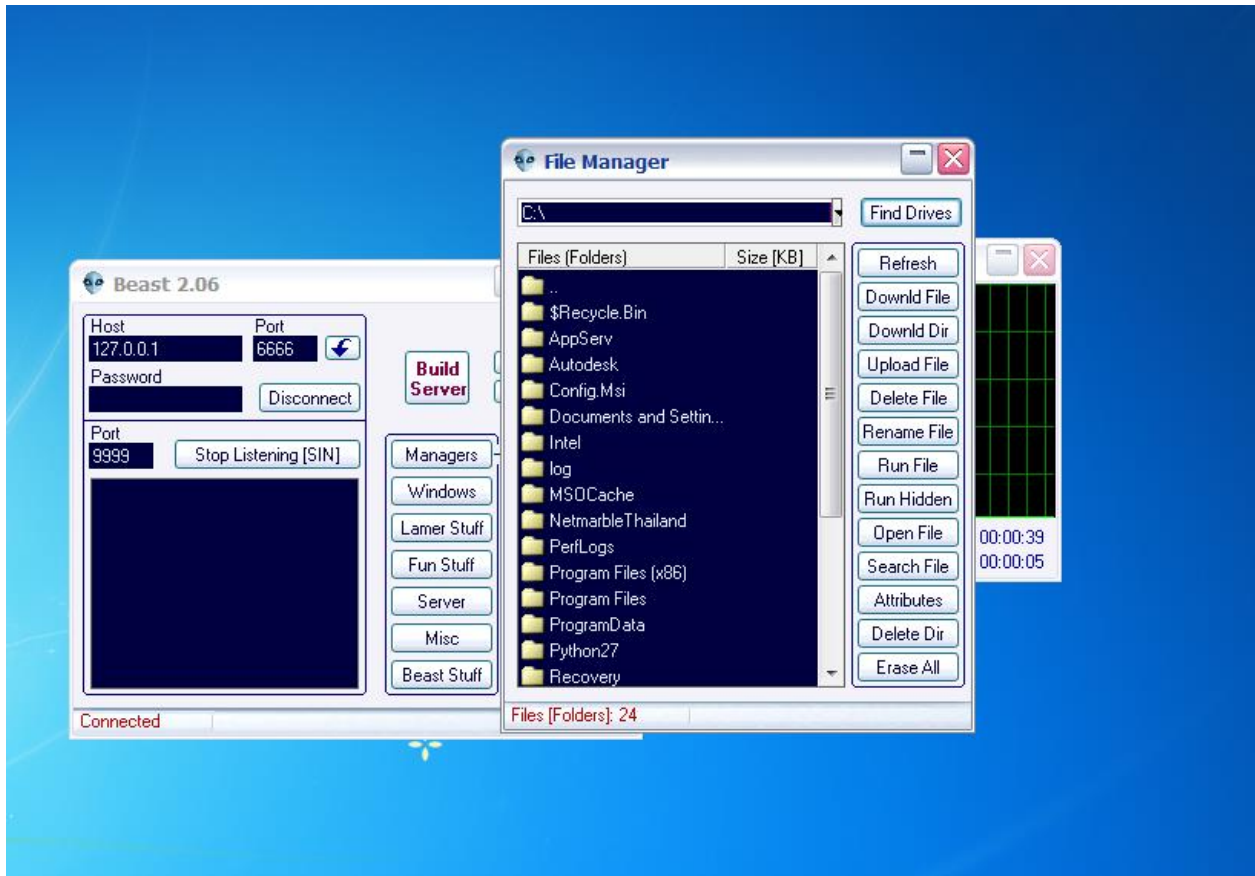
รูปที่ 15 : สังเกตไฟล์ .exe ที่ลงไว้ในเครื่องเป้าหมายจะหายไป



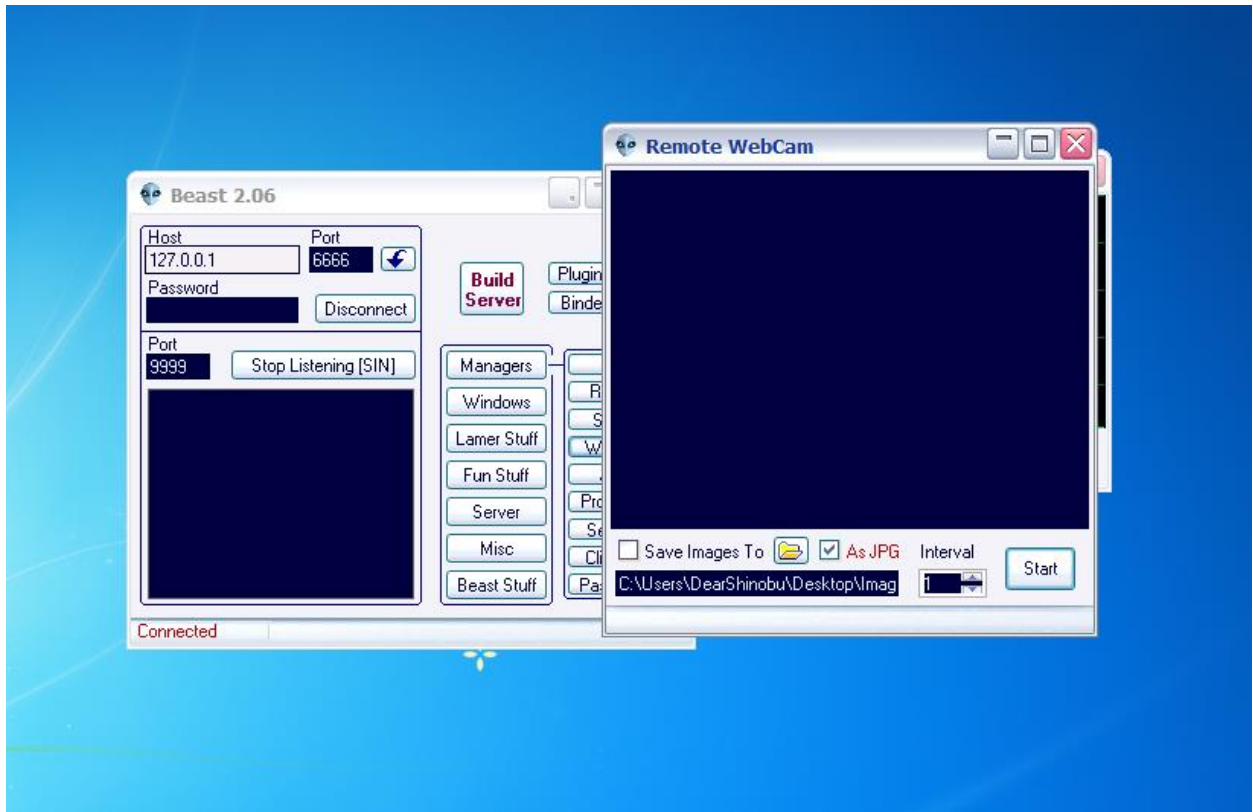
รูปที่ 16 : ในส่วนของเครื่องที่ใช้โจมตีเป้าหมาย กด **Start Listening [SIN]** รอสักครู่



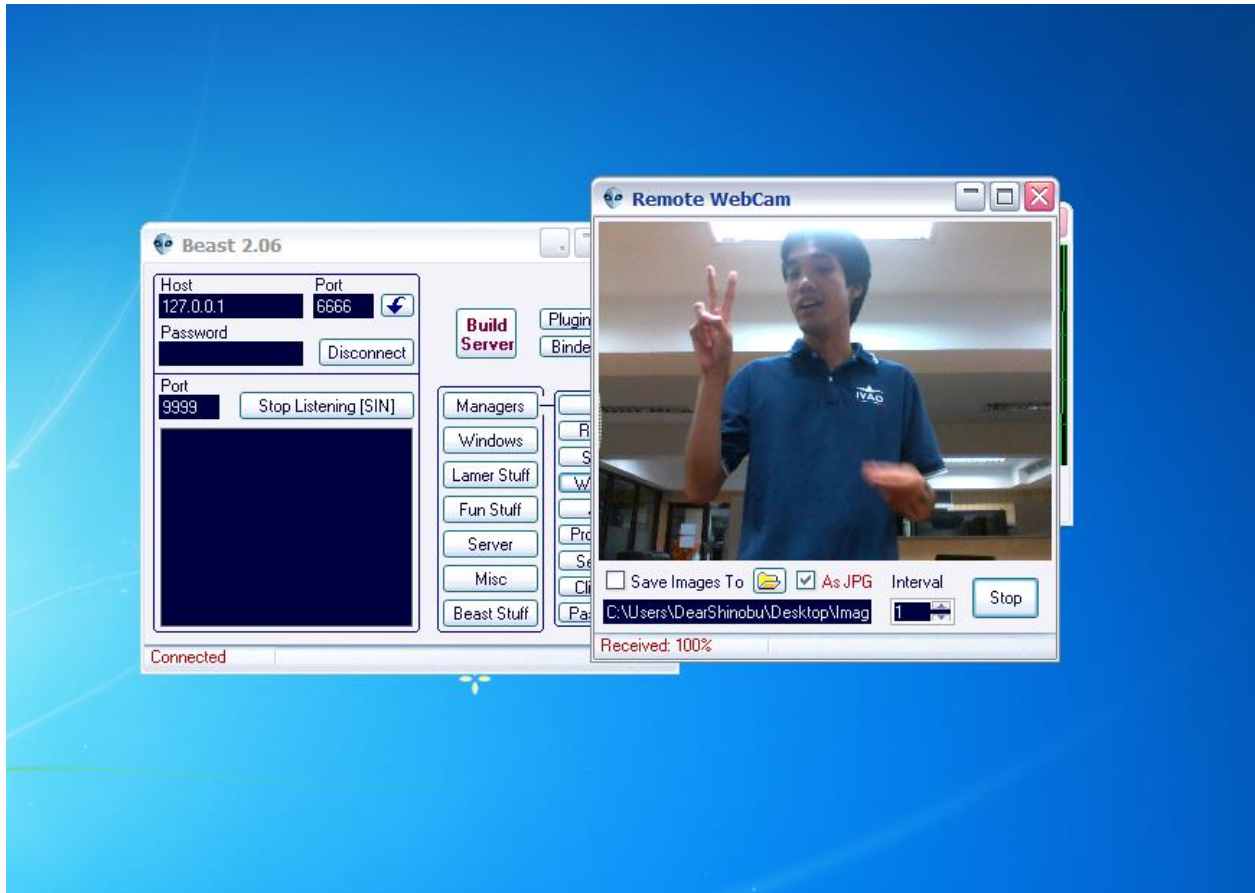
รูปที่ 17 : ระบบจะแสดงชื่อเครื่องที่เครื่องเป้าหมายที่ถูกโทรจันฝังไว้



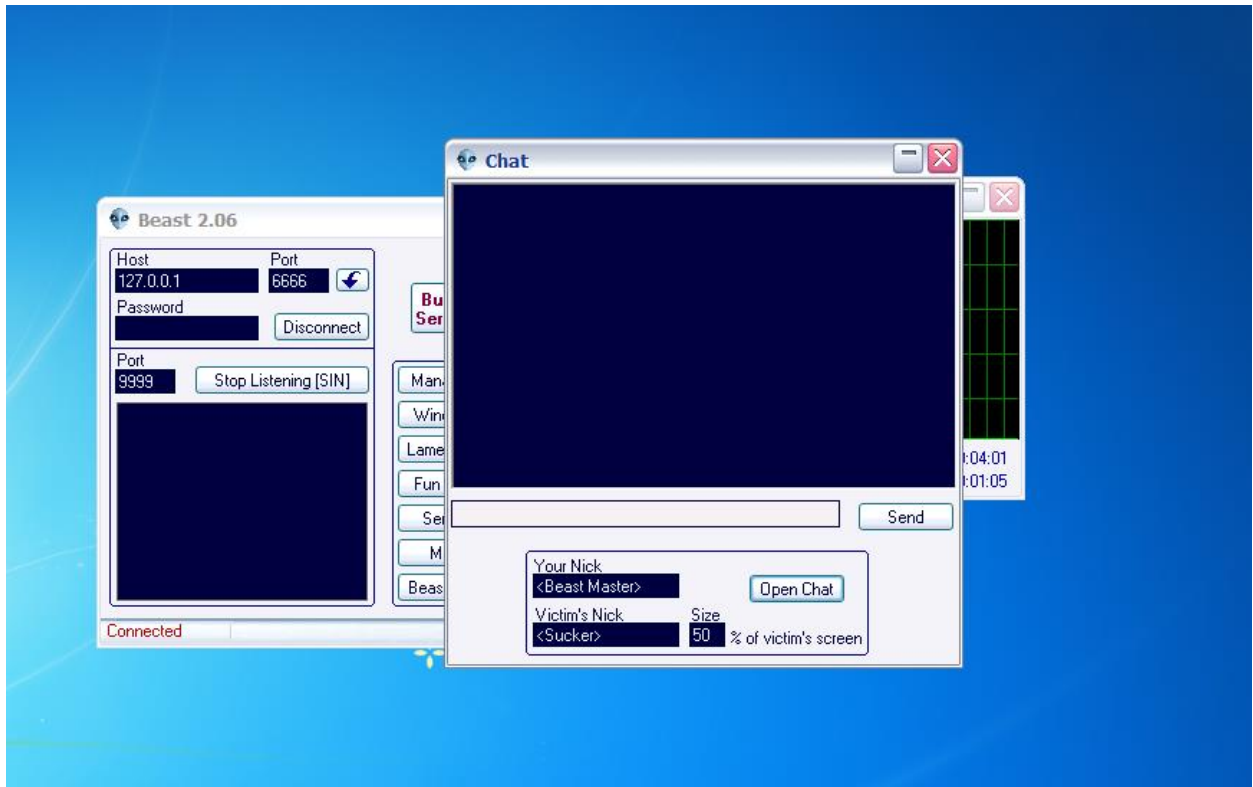
รูปที่ 18 : ทางขวาของโปรแกรม สามารถเลือกฟังก์ชันการใช้งานต่าง ๆ ได้ เช่น การเปิดกล้อง, เปิดตลาดซีดี, สถานะการประมวลผลของระบบ, ไฟล์ในไดเรกทอรีต่างๆ ฯลฯ



รูปที่ 19 : ในส่วนของการเปิดกล้อง โปรแกรมจะแสดงหน้าต่างสำหรับเปิดกล้องของเครื่องเป้าหมายขึ้นมา



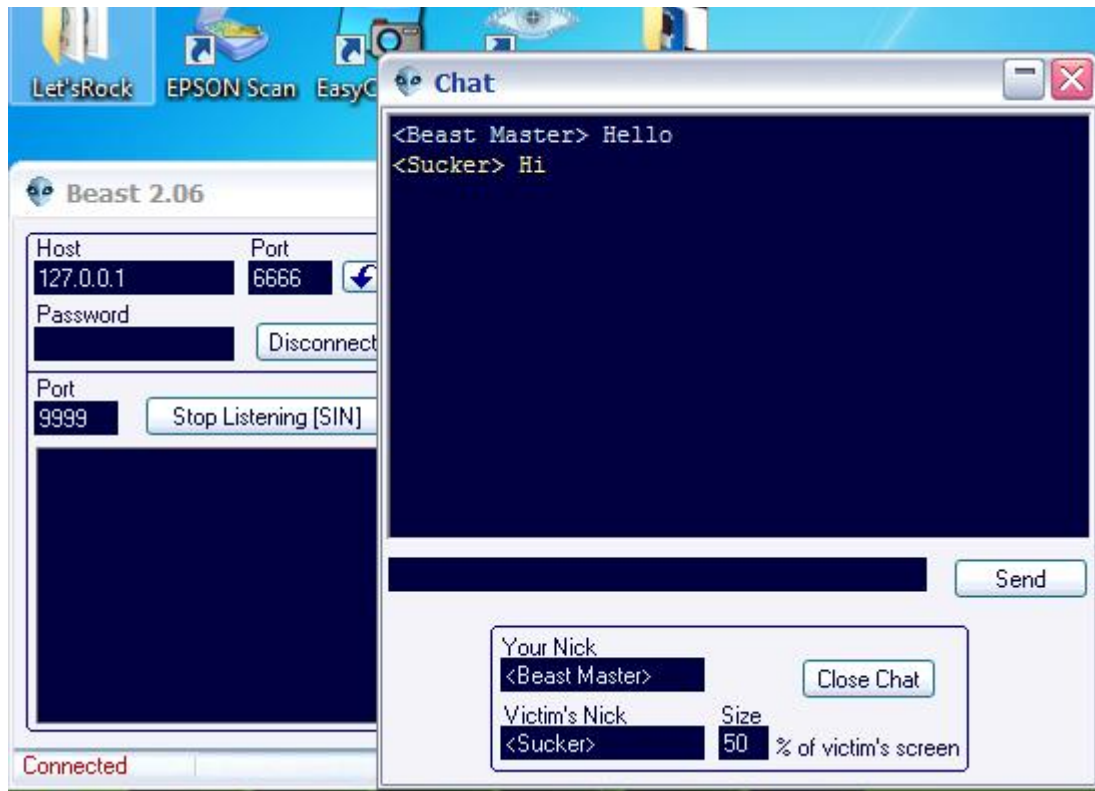
รูปที่ 20 : เมื่อกด **Start** โปรแกรมจะเปิดกล้องของเครื่องเป้าหมาย ดังภาพ



รูปที่ 21 : ในส่วนของการแชท โปรแกรมจะแสดงหน้าต่างขึ้นมาดังภาพ



รูปที่ 22 : ในส่วนของเครื่องเป้าหมาย หากผู้โจมตีส่งข้อความมาถึงเครื่องเป้าหมาย จะแสดงกล่องข้อความขึ้นมาบนหน้าจอ และสามารถตอบข้อความกลับไปได้



รูปที่ 23 : ในมุมมองของเครื่องผู้โจมตี จะสามารถกำหนดชื่อผู้ส่งได้