Security tool แบบโจมตี: **NetBus** (ม้าโทรจัน)

หมายเหตุ: ก่อนแตกไฟล์ NetBus ต้องปิด Filewall หรือ AntiVirus

553020422-3	นางสาวกานต์ชนก ขินสูงเนิน
553020425-7	นายคมกฤช ศรีสอน
553020460-5	นายมติชน สุโคตรพรหมมี
553020964-7	นายกฤษณ พิมพะนิตย์
553021022-4	นางสาวสมปอง สีหาราช

รายวิชา 322 376 INFORMATION AND COMMUNICATION TECHNOLOGY SECURITY

Section 3

Security tool แบบโจมตี: NetBus (ม้าโทรจัน)

หมายเหตุ: ก่อนแตกไฟล์ NetBus ต้องปิด Filewall หรือ AntiVirus

วิธีป้องกัน:

- เปิด Firewall ในระหว่างใช้อินเทอร์เน็ตทุกครั้ง
- ติดตั้งโปรแกรมแสกนไวรัส เช่น McAfee และรันไว้ขณะใช้อินเทอร์เน็ต

*วิธีป้องกันทั้ง 2 วิธีนี้ จะทำการดักจับและลบไฟล์ที่ติดไวรัสตัวนี้แบบอัตโนมัติ

การทำงนของ NetBus

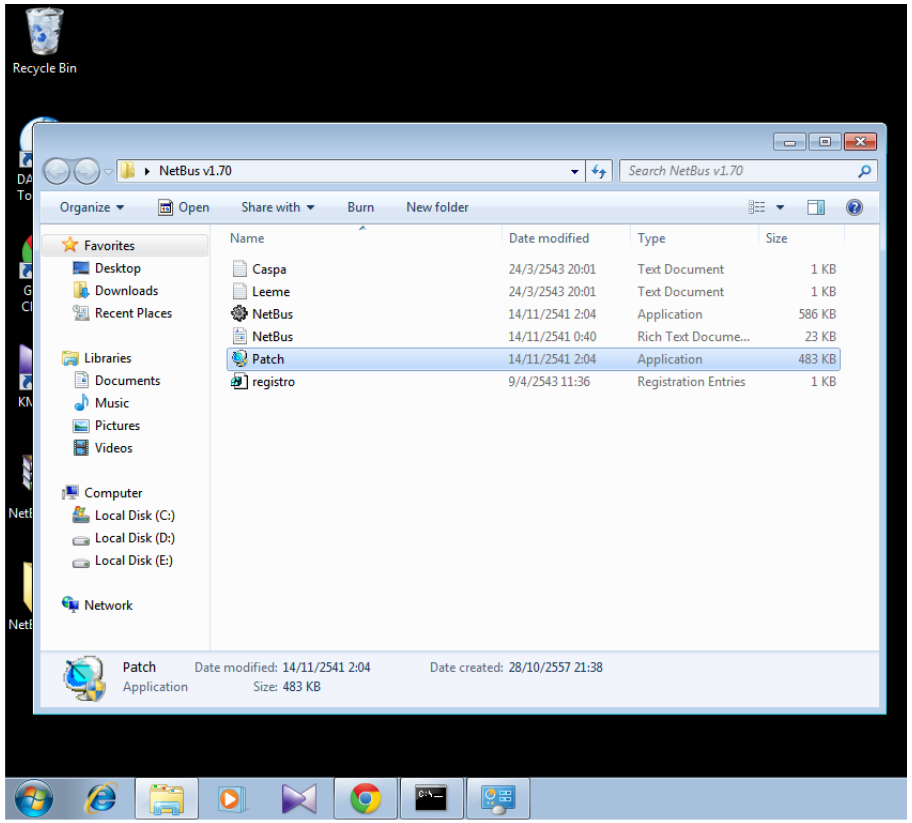
มีหลักการทำงานคล้ายโทรจัน เมื่อเครื่องเป้าหมายรัน pacth.exe ของ NetBus และผู้โจมตีรู้ IP Address ของเป้าหมาย ก็สามารถคุมเครื่องเป้าหมายได้ ซึ่งมีวิธีติดตั้ง และตัวอย่างการโจมตีดังต่อไปนี

Security tool แบบโจมตี: NetBus (ม้าโทรจัน)

หมายเหตุ: ก่อนแตกไฟล์ NetBus ต้องปิด Filewall หรือ AntiVirus

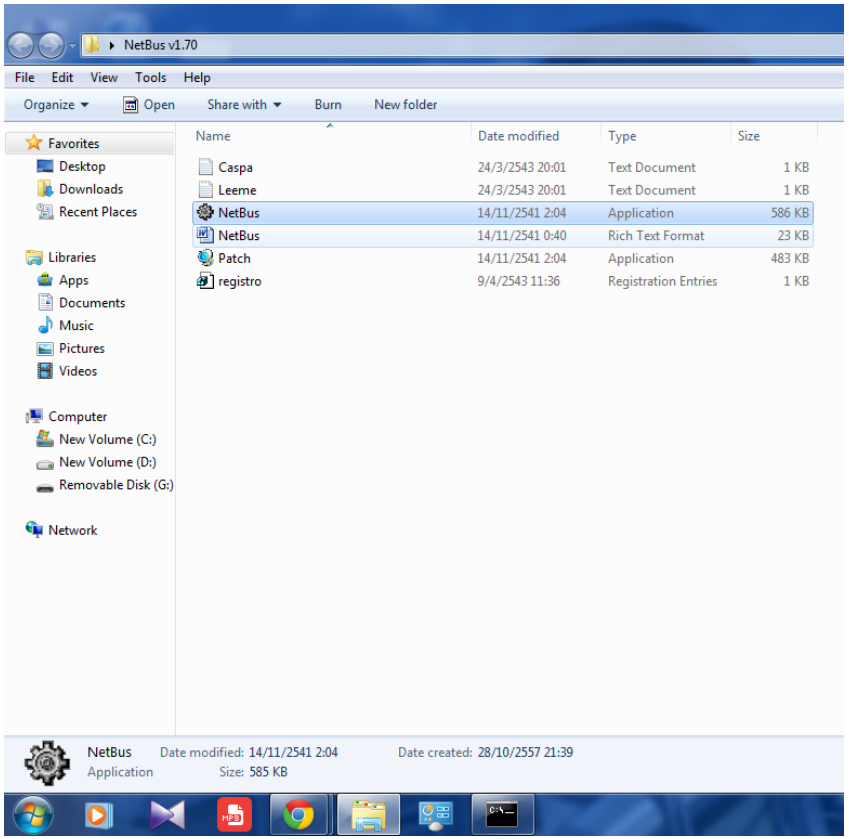
เครื่องเป้าหมาย

1. แตกไฟล์ NetBus ที่เครื่องเป้าหมาย จากนั้นติดตั้งโดยคลิกที่ไฟล์ Patch จะไม่ปรากฏหน้าต่างใด ๆ ขึ้น



เครื่องควบคุม

1. แตกไฟล์ NetBus ที่เครื่องควบคุม จากนั้นคลิกที่ไฟล์ NetBus

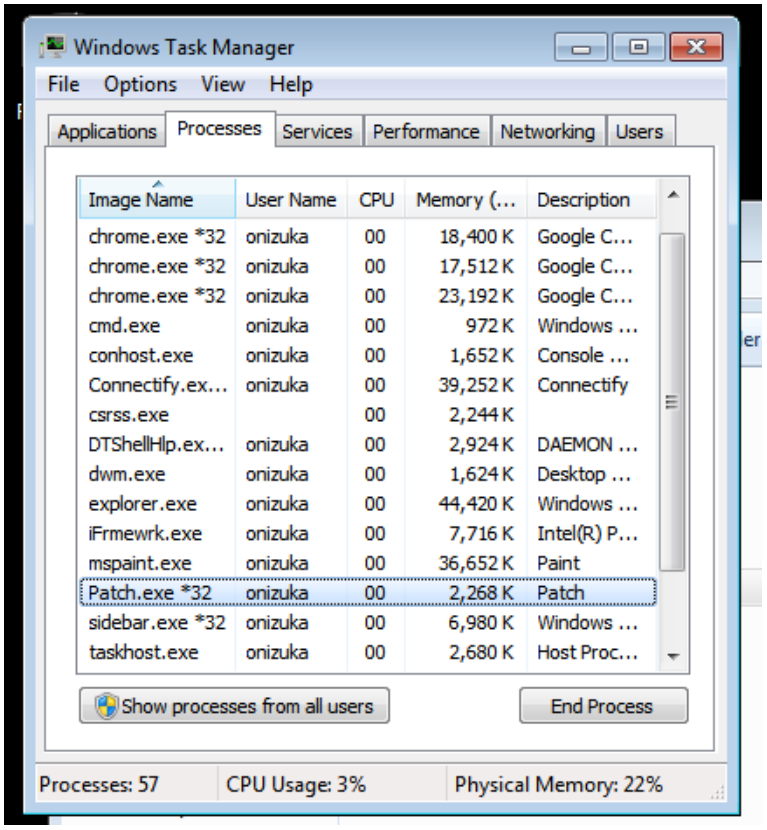


Security tool แบบโจมตี: NetBus (ม้าโทรจัน)

หมายเหตุ: ก่อนแตกไฟล์ NetBus ต้องปิด Filewall หรือ AntiVirus

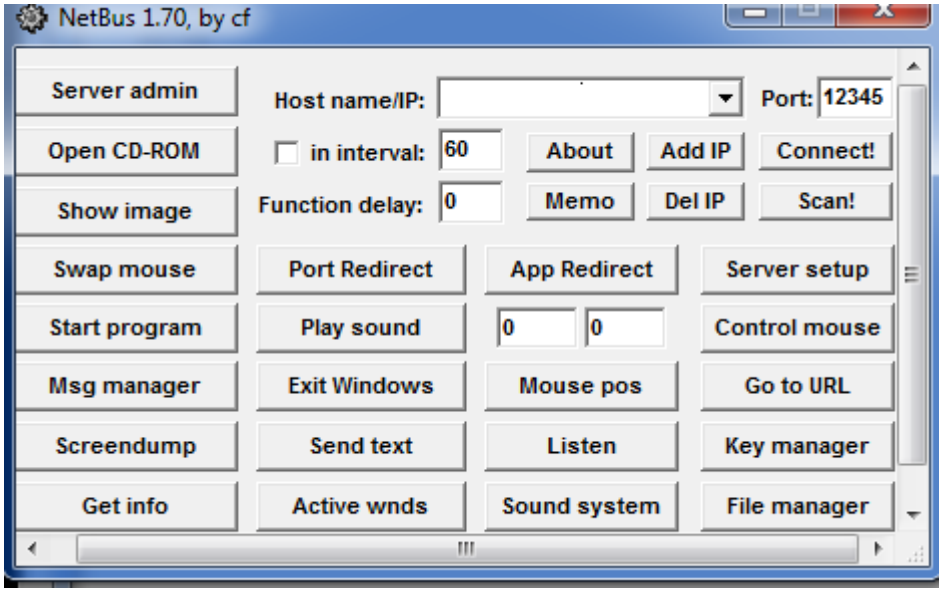
เครื่องเป้าหมาย

2. แต่ Patch.exe ได้เริ่มทำงานแล้ว สามารถตรวจสอบได้โดย ใช้โปรแกรม Windows Task Manager จะเห็นว่า Patch.exe กำลังรันอยู่



เครื่องควบคุม

2. จะปรากฏโปรแกรม NetBus ที่จะใช้ควบคุมเครื่องเป้าหมาย

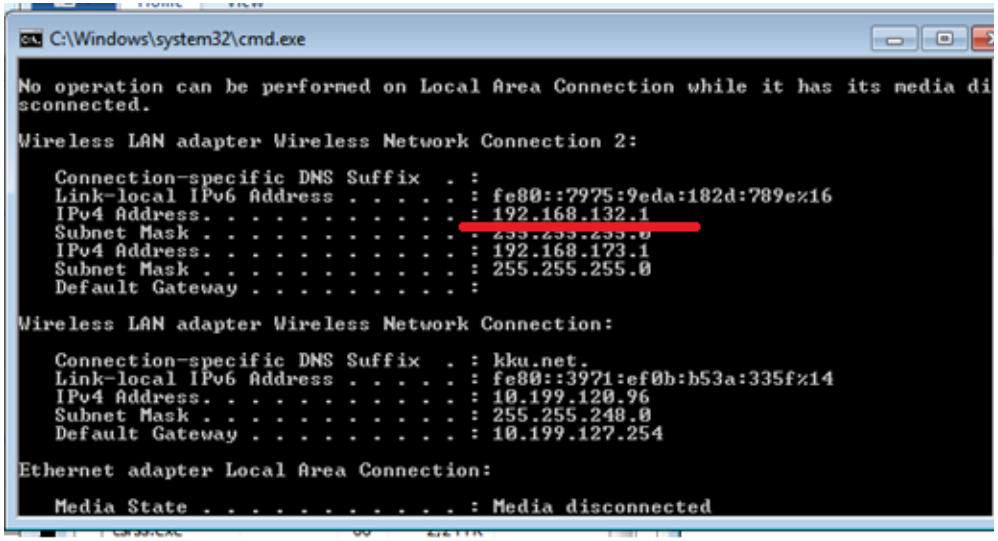


Security tool แบบโจมตี: NetBus (ม้าโทรจัน)

หมายเหตุ: ก่อนแตกไฟล์ NetBus ต้องปิด Filewall หรือ AntiVirus

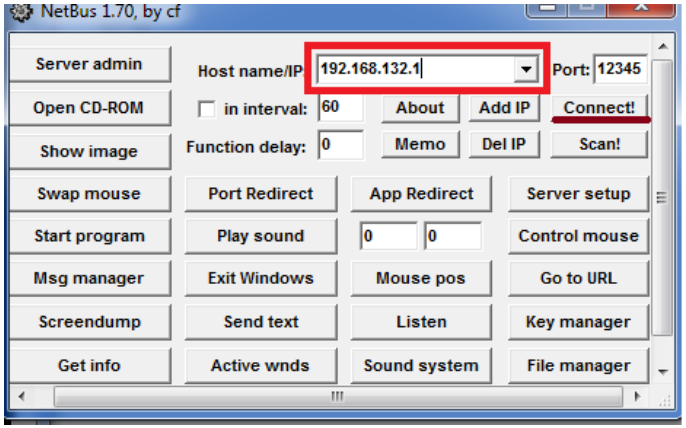
เครื่องเป้าหมาย

3. เช็ค IP Address เครื่องเป้าหมาย

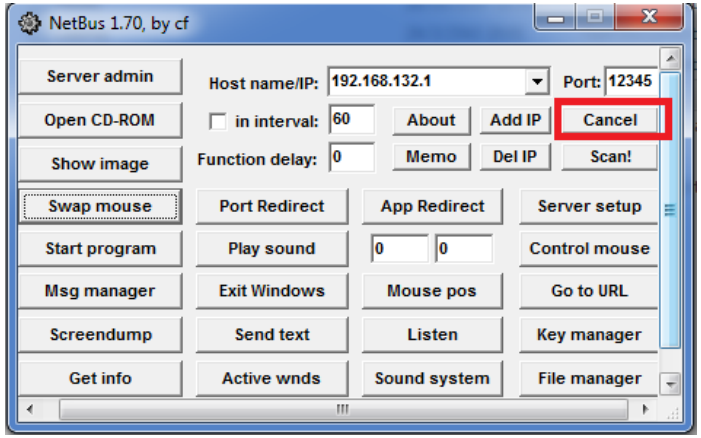


เครื่องควบคุม

3. ฝั่งเครื่องควบคุม นำ IP Address เครื่องเป้าหมาย ใส่ในช่อง Host Name/IP แล้วกด Connect! เพื่อโจมตี



ถ้าเชื่อมต่อเครื่องเป้าหมายได้ ที่ปุ่ม Connect! จะเปลี่ยนเป็น Cancel



Security tool แบบโจมตี: NetBus (ม้าโทรจัน)

หมายเหตุ: ก่อนแตกไฟล์ NetBus ต้องปิด Filewall หรือ AntiVirus

เครื่องเป้าหมาย

เครื่องเป้าหมายยังคงทำงานปกติ

Security tool แบบโจมตี: NetBus (ม้าโทรจัน)

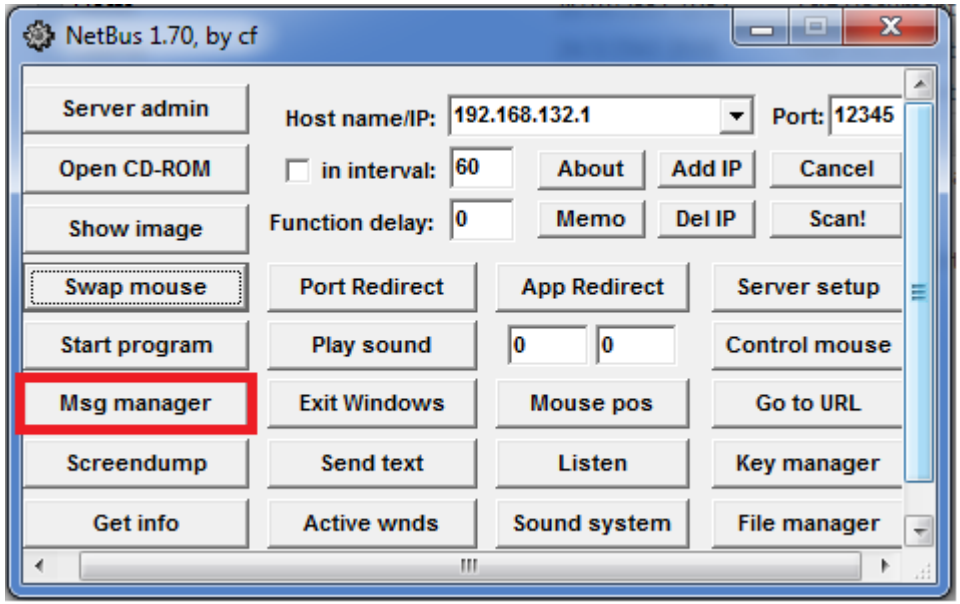
หมายเหตุ: ก่อนแตกไฟล์ NetBus ต้องปิด Filewall หรือ AntiVirus

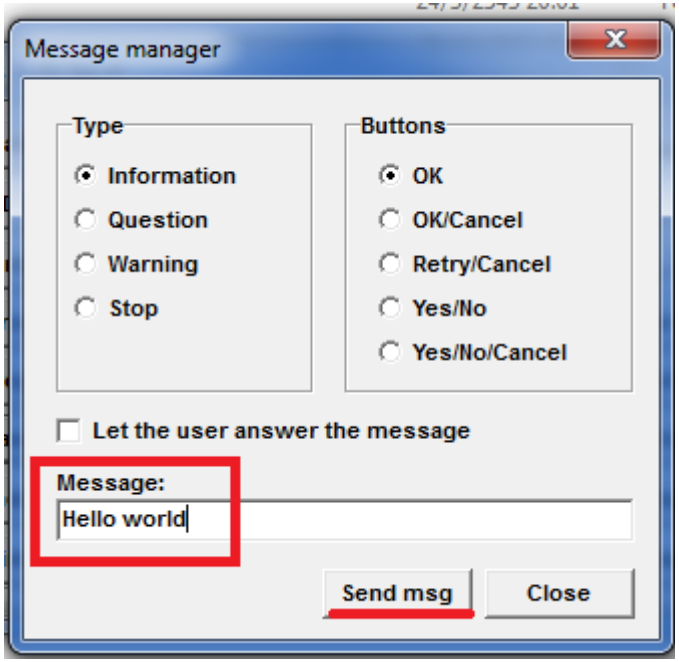
ตัวอย่างการโจมตีที่ 1

เครื่องควบคุม

เมื่อต้องการให้แสดง Message Box ที่เครื่องเป้าหมาย

กดที่ปุ่ม Msg manager จะปรากฏหน้าต่าง Message manager จากนั้นระบุข้อความที่ต้องการ แล้วกด Send msg



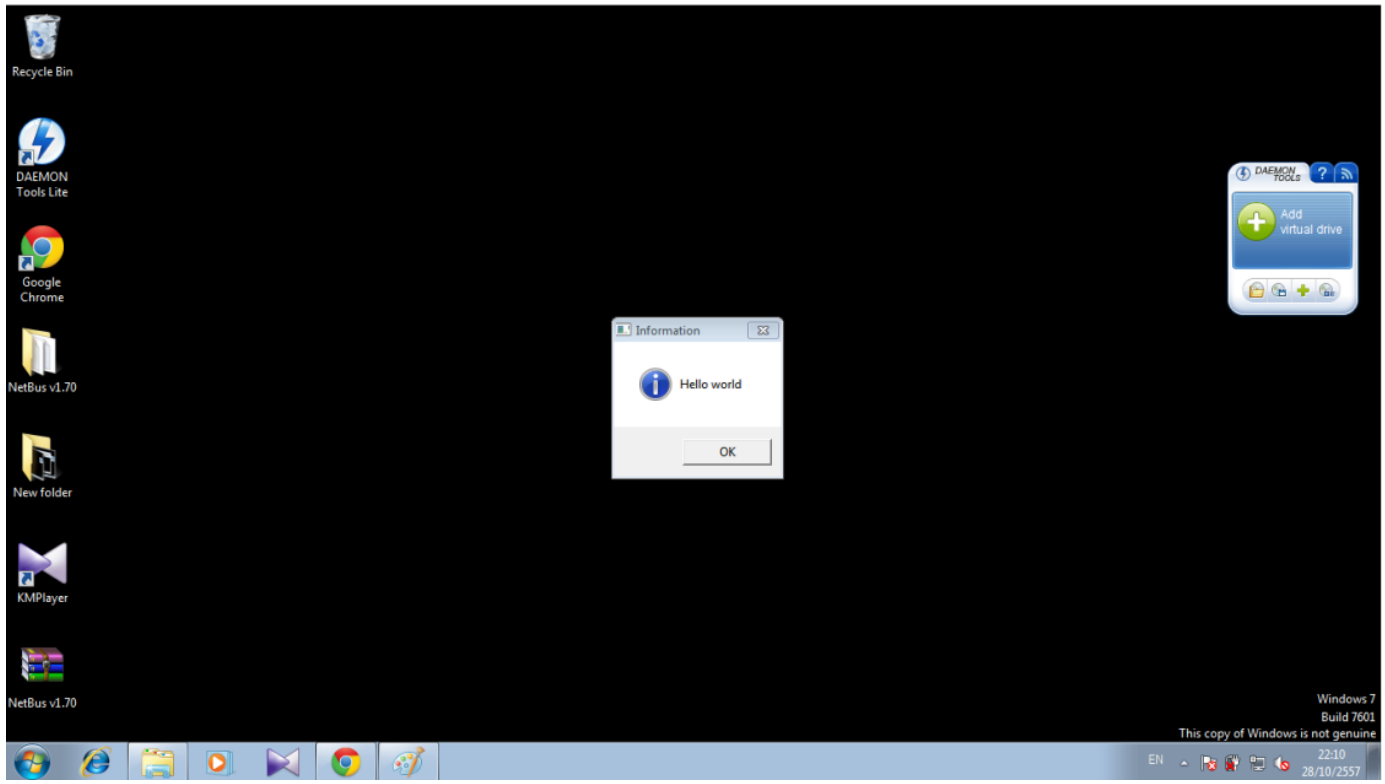


Security tool แบบโจมตี: NetBus (ม้าโทรจัน)

หมายเหตุ: ก่อนแตกไฟล์ NetBus ต้องปิด Filewall หรือ AntiVirus

เครื่องเป้าหมาย

จะปรากฏ Message Box ที่เครื่องเป้าหมาย



Security tool แบบโจมตี: NetBus (ม้าโทรจัน)

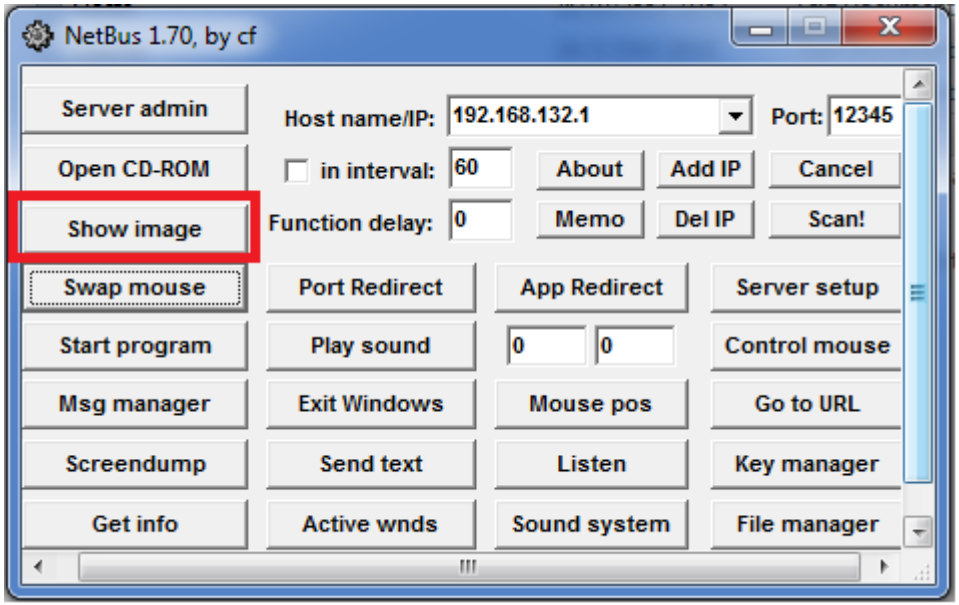
หมายเหตุ: ก่อนแตกไฟล์ NetBus ต้องปิด Filewall หรือ AntiVirus

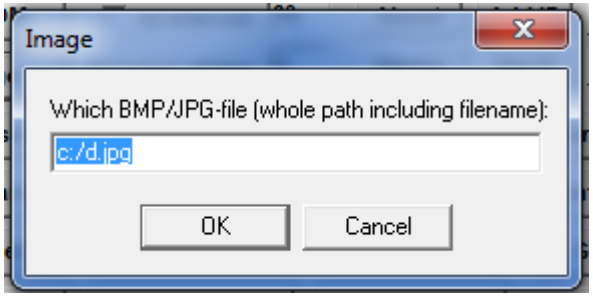
ตัวอย่างการโจมตีที่ 2

เครื่องควบคุม

เมื่อต้องการให้แสดงรูปภาพที่เครื่องเป้าหมาย

กดที่ปุ่ม Show image จะปรากฏหน้าต่าง Image จากนั้นระบุที่อยู่ของไฟล์รูปภาพนั้น แล้วกด OK





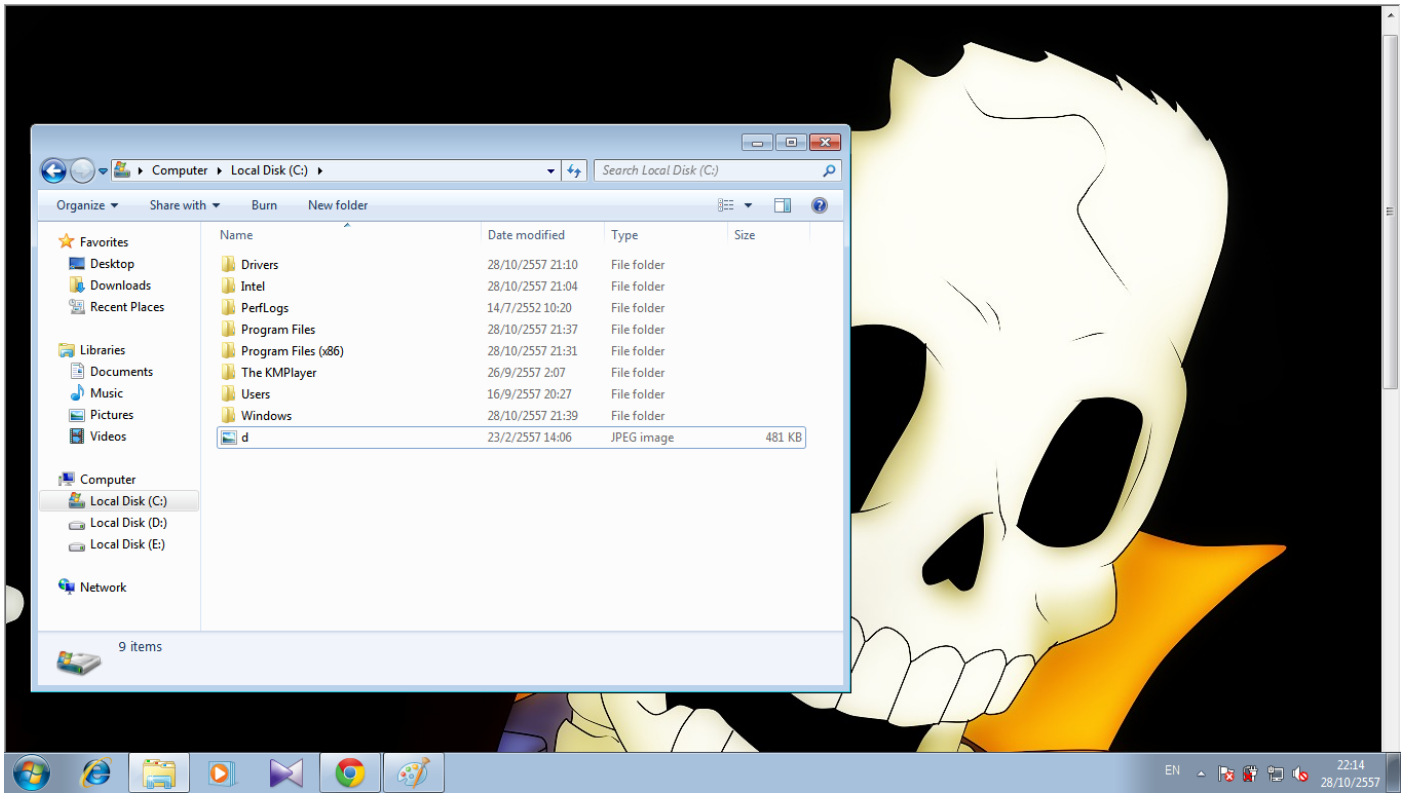
*หมายเหตุ: ไฟล์รูปภาพเป็นไฟล์ที่มีอยู่ที่เครื่องเป้าหมาย

Security tool แบบโจมตี: NetBus (ม้าโทรจัน)

หมายเหตุ: ก่อนแตกไฟล์ NetBus ต้องปิด Filewall หรือ AntiVirus

เครื่องเป้าหมาย

จะปรากฏรูปภาพขนาดเต็มจอที่เครื่องเป้าหมาย



*หมายเหตุ: ณ ที่นี้ ปรากฏหน้าต่างโฟลเดอร์ที่เก็บไฟล์รูปภาพ เพื่อแสดงให้เห็นว่า รูปภาพในเครื่องเป้าหมาย

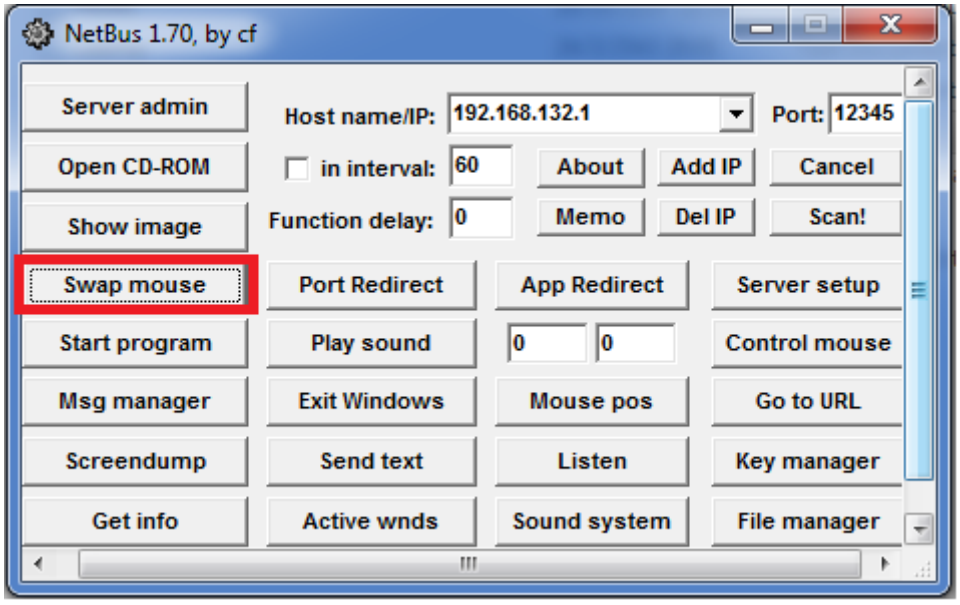
Security tool แบบโจมตี: NetBus (ม้าโทรจัน)

หมายเหตุ: ก่อนแตกไฟล์ NetBus ต้องปิด Filewall หรือ AntiVirus

ตัวอย่างการโจมตีที่ 3

เครื่องควบคุม

ต้องสลับการคลิกเมาส์ กดที่ปุ่ม Swap mouse เมื่อผู้ใช้งานเครื่องเป้าหมายคลิกซ้ายจะกลายเป็นคลิกขวา และคลิกขวาจะกลายเป็นคลิกซ้าย



Security tool แบบโจมตี: NetBus (ม้าโทรจัน)

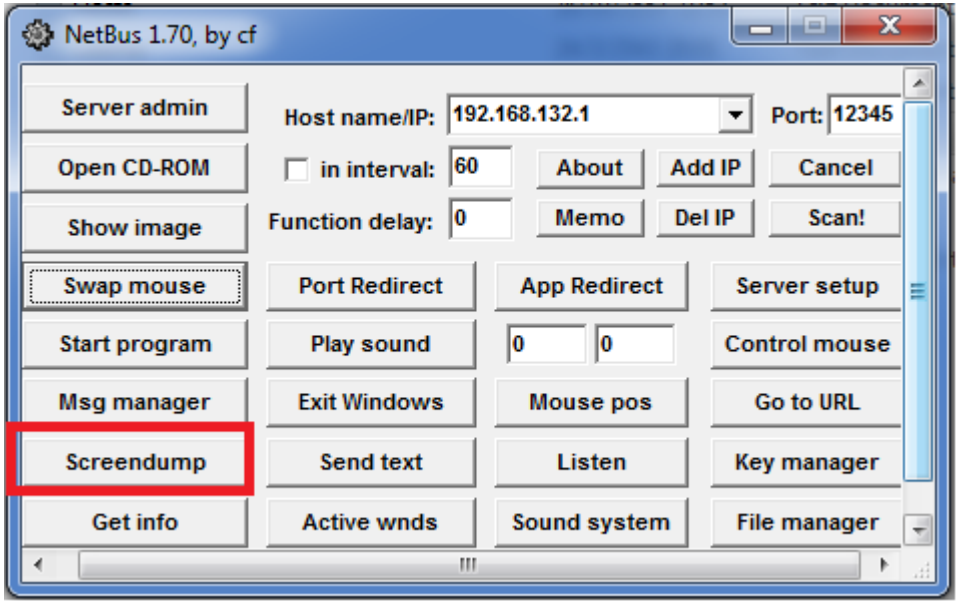
หมายเหตุ: ก่อนแตกไฟล์ NetBus ต้องปิด Filewall หรือ AntiVirus

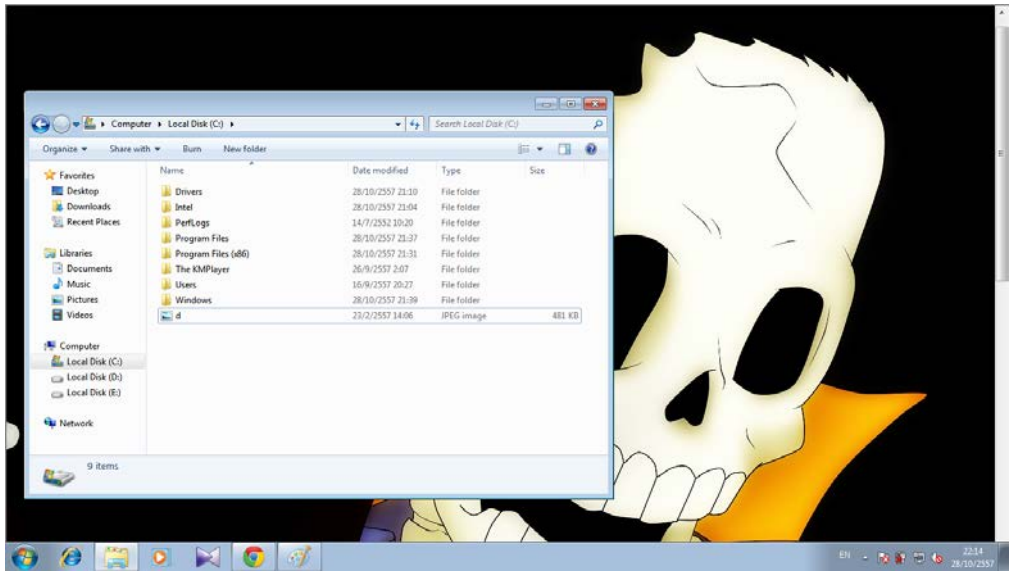
ตัวอย่างการโจมตีที่ 4

เครื่องควบคุม

เมื่อต้องการดูว่าตอนนี้เครื่องเป้าหมายรันอะไรไว้บนหน้าจอบ้าง (เพื่อเตรียมการโจมตีขั้นต่อไป)

กดที่ปุ่ม Screendump จะปรากฏหน้าจอเดสท์ท็อปของเครื่องเป้าหมาย





ที่มา : http://writer.dek-d.com/meromo1983/story/viewlongc.php?id=225167&chapter=116