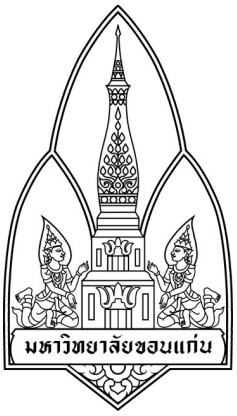


รายงาน

เรื่อง Social Engineering Toolkits

จัดทำโดย

1. นายณัฐพงศ์	แสนแก้ว	573020416-0 sec.2 Group 55
2. นายณัฐวุฒิ	กรุดมินบุรี	573020417-8 sec.2 Group 55
3. นายศักดิ์ดา	ประทุมชมภู	573020438-0 sec.2 Group 56
4. นางสาวอัญมณี	ผาจวง	573020451-8 sec.2 Group 56
5. นายศรัณญ์	สาพรหม	573020683-7 sec.2 Group 57
6. นางสาวธัญยพร	วาสสามัคคี	573021143-4 sec.2 Group 57

เสนอ

อ. รศ.ดร.จักรชัย โสอินทร์

รายงานนี้เป็นส่วนหนึ่งของการศึกษาวิชา 322 376 ชื่อวิชา INFORMATION AND COMMUNICATION TECHNOLOGY SECURITY

ภาคเรียน 1 ปีการศึกษา 2559

ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์

มหาวิทยาลัยขอนแก่น

หลักการและเหตุผล

ปัจจุบัน ภัยร้ายเข้ามาหาเราได้ในหลายรูปแบบ และล้วนเป็นภัยใกล้ตัว ที่หากไม่ไตร่ตรองให้ดี อาจตกเป็นเหยื่อของภัยดังกล่าวอย่างง่ายดาย ข่าวมากมาย เกี่ยวกับภัยใกล้ตัวในรูปแบบต่างๆ เช่น ภัยทางโทรศัพท์ ภัยทางอินเตอร์เน็ต หรือภัยจากการถูกโจรกรรมข้อมูลไปใช้ในทางที่ไม่ดี เป็นต้น การโจรกรรมข้อมูลส่วนบุคคล คือการการขโมยข้อมูลส่วนบุคคลของผู้อื่นไปใช้ฉ้อโกงหรือก่ออาชญากรรมอื่นๆ เช่น นำข้อมูลของเราไปใช้ทำบัตรเครดิต กู้เงิน หรือเปิดบัญชีใหม่ เป็นต้น จากนั้นก็สร้างหนี้ก้อนโตไว้ในชื่อของเรา ซึ่งกว่าที่จะแก้ไขปัญหาดังกล่าว ก็อาจจะเสียประวัติ ด้วยเหตุนี้คณะผู้จัดทำจึงได้ศึกษา โปรแกรม Kali Linux และโปรแกรม Social Engineering Toolkit เพื่อไม่ให้ตกเป็นเหยื่อของผู้ประสงค์ร้าย ซึ่งอาจจะกระทำได้หลากหลายวิธี เช่น Hacking, Cracking แต่วิธีอีกวิธีหนึ่งที่เป็นที่นิยมเช่นกันคือวิธีที่เรียกว่า Trojan Horse คณะผู้จัดทำจึงได้ศึกษาการโจมตีแบบ Trojan Horse

วัตถุประสงค์

1.เพื่อศึกษาวิธีการโจมตีเครื่องคอมพิวเตอร์ด้วย Trojan Horse

2. เพื่อศึกษาวิธีการป้องกันเครื่องคอมพิวเตอร์จาก Trojan Horse

3. เพื่อที่จะนำแนวทางป้องกันไปประยุกต์ใช้ได้ในชีวิตประจำวัน

ประโยชน์ที่คาดว่าจะได้รับ

1. ทราบถึงแนวทางการโจมตีด้วย Trojan Horse

2. ทราบถึงแนวทางการป้องกันการโจมตีด้วย Trojan Horse

3. สามารถนำแนวทางป้องกันไปประยุกต์ใช้ได้ในชีวิตประจำวัน

เครื่องมือและโปรแกรมที่ใช้ในการทดสอบ

1. Kali Linux 2.0

ภาพที่ 1 Kali Linux 2.0

Kali Linux 2.0 หรือโค้ดเนม “Kali Sana” เป็นแพลทฟอร์มรันบนระบบปฏิบัติการ Debian Jesse สำหรับใช้เจาะระบบคอมพิวเตอร์เพื่อตรวจหาช่องโหว่โดยเฉพาะ ซึ่งมาพร้อมกับชุดทดสอบเจาะระบบมากกว่า 100 รายการ รวมทั้งมีระบบการวิเคราะห์เชิงสถิติ การแฮ็ค และวิศวกรรมย้อนกลับ (Reverse Engineering) ในเวอร์ชัน 2.0 ล่าสุดนี้ ได้ทำการออกแบบอินเตอร์เฟสใหม่ จัดกลุ่มเครื่องมือ และเมนูแสดงผลต่างๆเพื่อให้ใช้งานได้สะดวกคล่องตัวมากยิ่งขึ้น

2. Social Engineering Toolkits (SET)

ภาพที่ 2 Social Engineering Toolkit (SET)

โปรแกรม Social Engineering Toolkit (SET) เป็นโปรแกรมที่ใช้ในโจมตีแบบวิศวกรรมสังคมจะเกี่ยวกับการหลอกให้บางคนหลงกลเพื่อเข้าระบบ เช่น การหลอกถามรหัสผ่าน การหลอกให้ส่งที่สำคัญให้ ซึ่งการโจมตีประเภทนี้ไม่จำต้องใช้ความรู้ความชำนาญเกี่ยวกับคอมพิวเตอร์หรือการเจาะระบบเลย วิศวกรรมสังคมเป็นจุดอ่อนที่ป้องกันยากเพราะเกี่ยวข้องกับคน

3. Oracle Virtual Box

ภาพที่ 3 Oracle Virtual Box

VirtualBox (ชื่อเต็มคือ Oracle VM VirtualBox) เป็นโปรแกรมฟรีแวร์สำหรับจำลองระบบคอมพิวเตอร์ ได้ออกอัปเดทเวอร์ชันใหม่คือ VirtualBox 3.2.12 Build 68302 เมื่อวันที่ 30-Nov-2010 โดยในเวอร์ชันนี้สามารถรองรับ Ubuntu 10.10 และ Fedora 14

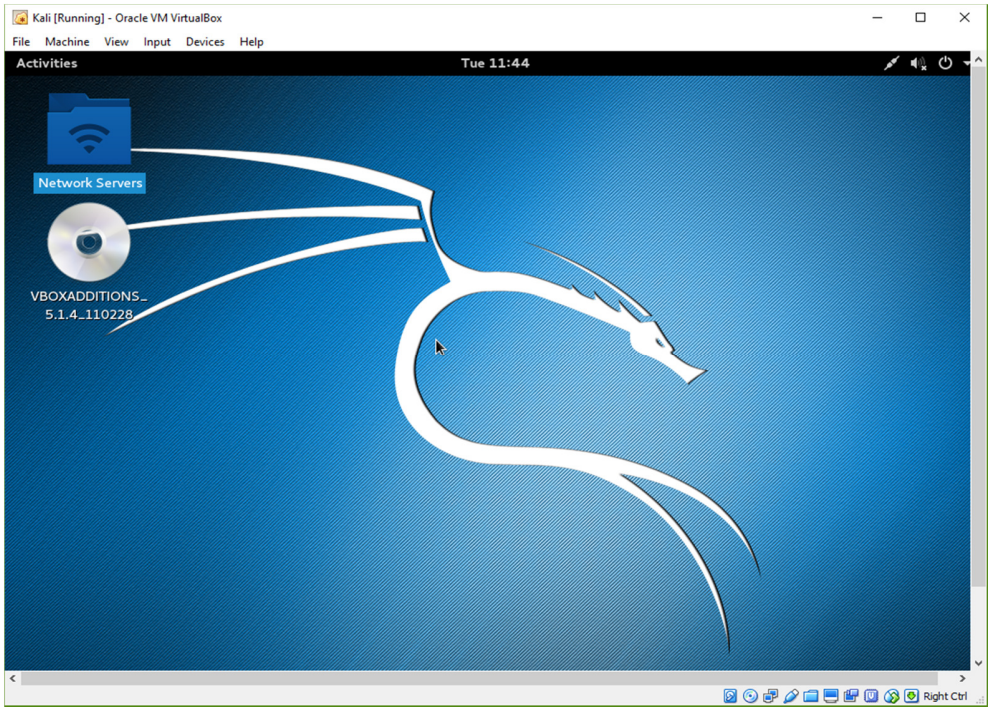
VirtualBox เป็นซอฟต์แวร์สำหรับใช้ทำการจำลองระบบคอมพิวเตอร์ (Virtualization) บนระบบ x86 และ AMD64/Intel64 ลักษณะเดียวกับโปรแกรม VMware Workstation (เป็นโปรแกรมเชิงพานิชย์ต้องซื้อจึงจะใช้งานได้เต็มฟังก์ชัน) และ VMware Player 3.0 (สามารถใช้งานได้ฟรี) ของVMware หรือโปรแกรม Virtual PC ของ Microsoft ซึ่งสามารถใช้งานได้ฟรี และ Windows Virtual PC ของ Microsoft ซึ่งใช้งานได้ฟรีแต่จะมีเฉพาะในWindows 7 ร่น Professional, Enterprise และ Ultimate

VirtualBox เป็นซอฟต์แวร์แบบ Open Source พัฒนาโดย Oracle (ก่อนหน้านี้เป็น Sun Microsystems ซึ่งปัจจุบันถูกซื้อกิจการโดย Oracle)สามารถใช้งานได้ฟรีโดยไม่มีค่าใช้จ่ายภายใต้ไลเซนส์แบบ GNU General Public License (GPL) เป็นซอฟต์แวร์ที่มีประสิทธิภาพสูงรองรับการใช้งานได้ทั้งในเอนเทอร์ไพรส์ (Enterprise) และการใช้งานภายในบ้าน และยังมีฟีเจอร์ให้ใช้งานหลากหลายและที่สำคัญเป็นโซลูชั่นระดับมืออาชีพที่ใช้งานได้ฟรี

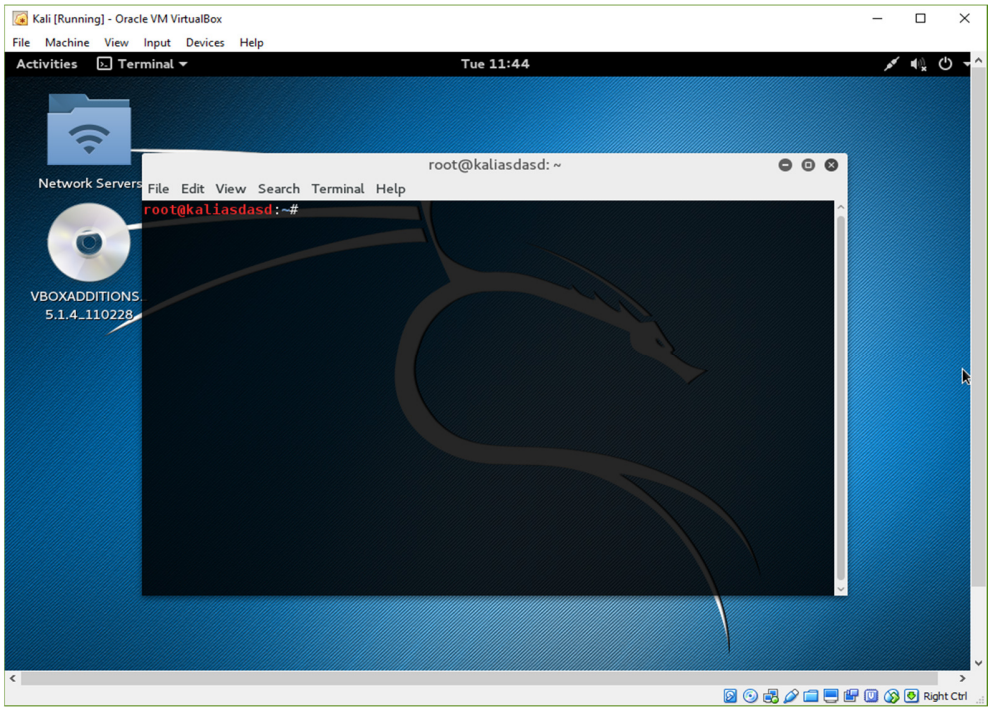
VirtualBox คือโปรแกรมที่ใช้ในการจำลองเครื่องคอมพิวเตอร์ขึ้นมาอีกเครื่องหนึ่งโดยการแบ่งทรัพยากรจากระบบหลักไปใช้เช่น CPU,RAM,VGA,HDD โดยจุดมุ่งหมายหลักของโปรแกรมนี้คือการติดตั้งระบบปฏิบัติการขึ้นมาอีกตัวหนึ่งเพื่อใช้งานที่แตกต่างกันไป สามารถใช้งานได้ Windows, Mac, Linux

ขั้นตอนการใช้งาน

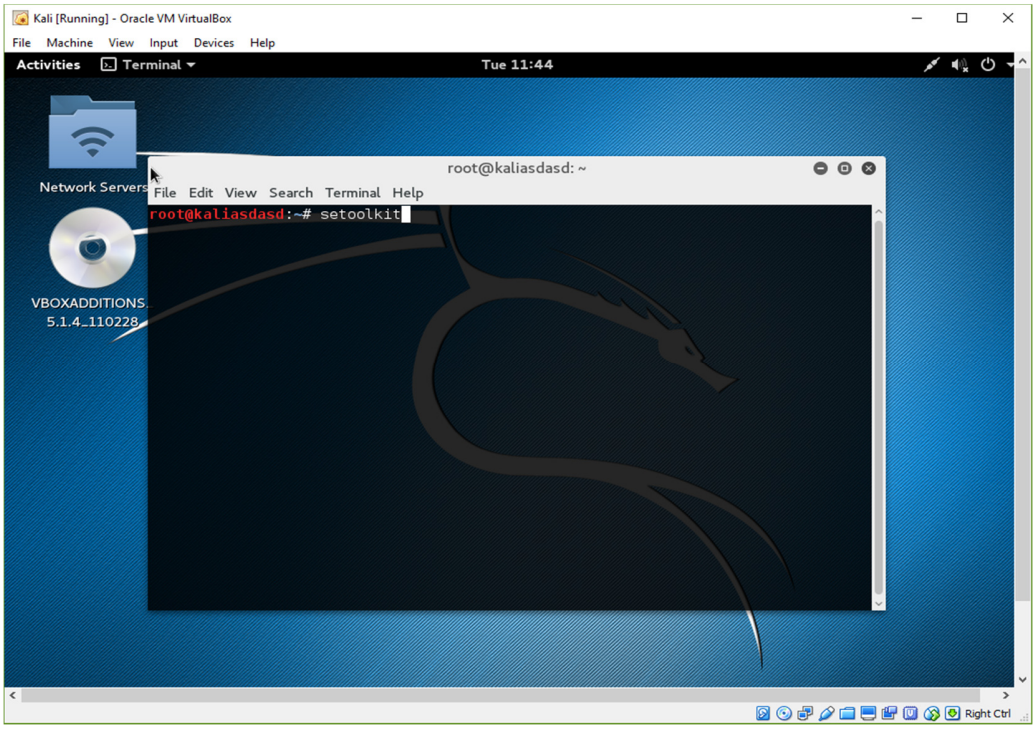
1. การสร้างไฟล์ Payload ด้วย Social Engineering Toolkit (SET)



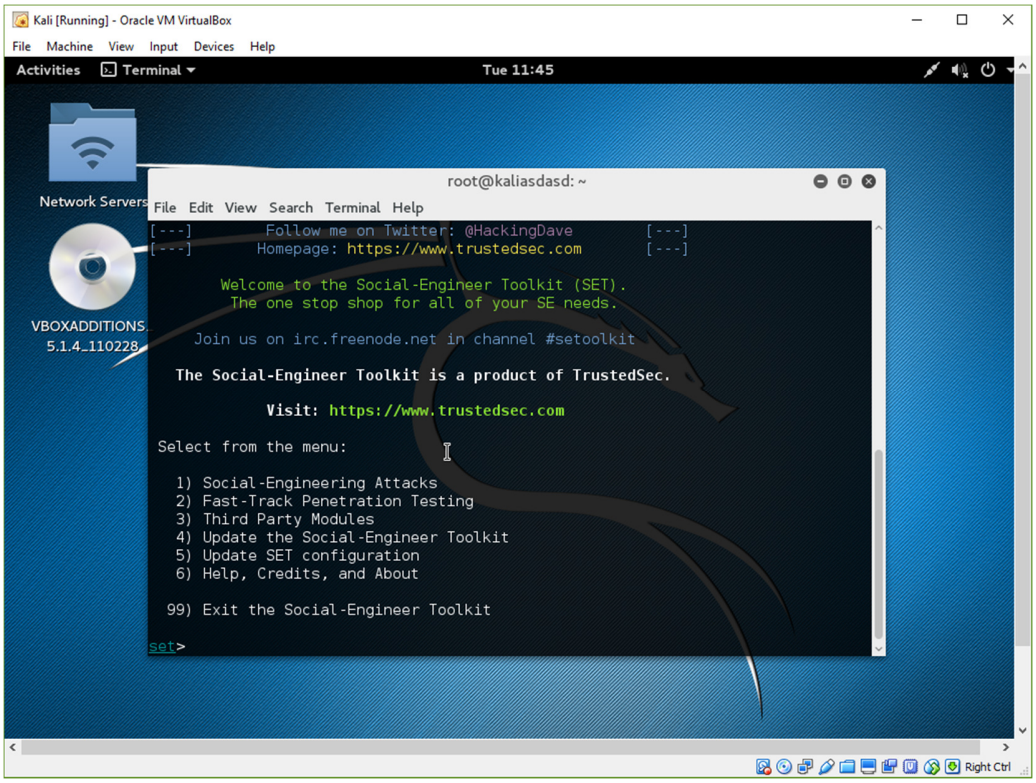
1.1 เปิดโปรแกรม Oracle VM VirtualBox จากนั้นทำการบูต Kali Linux ขึ้นมา



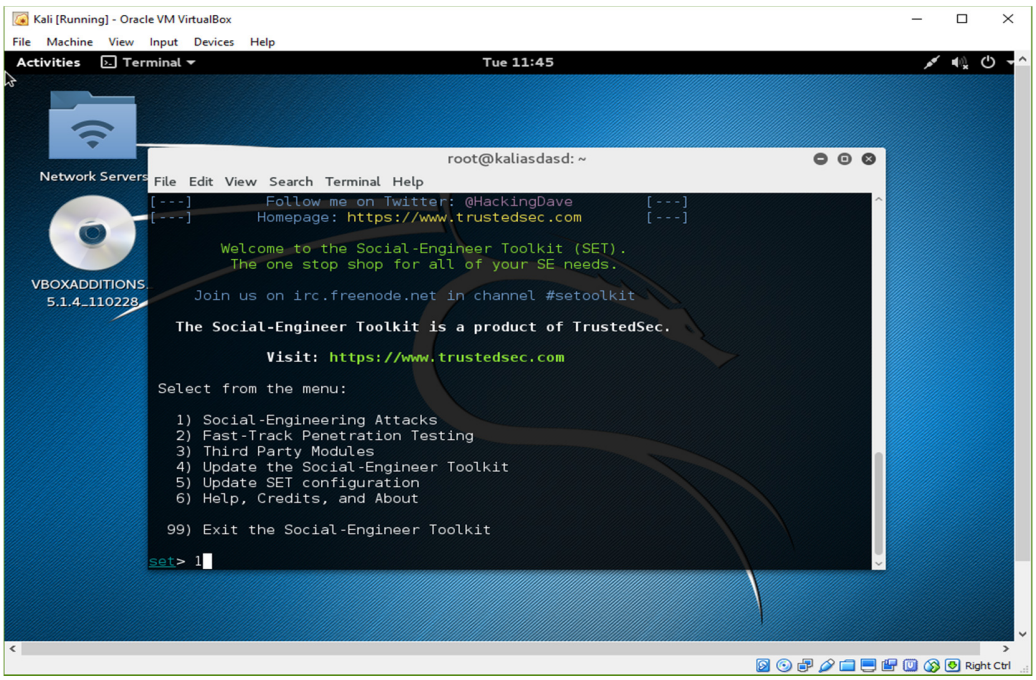
1.2. เรียกใช้งาน Terminal



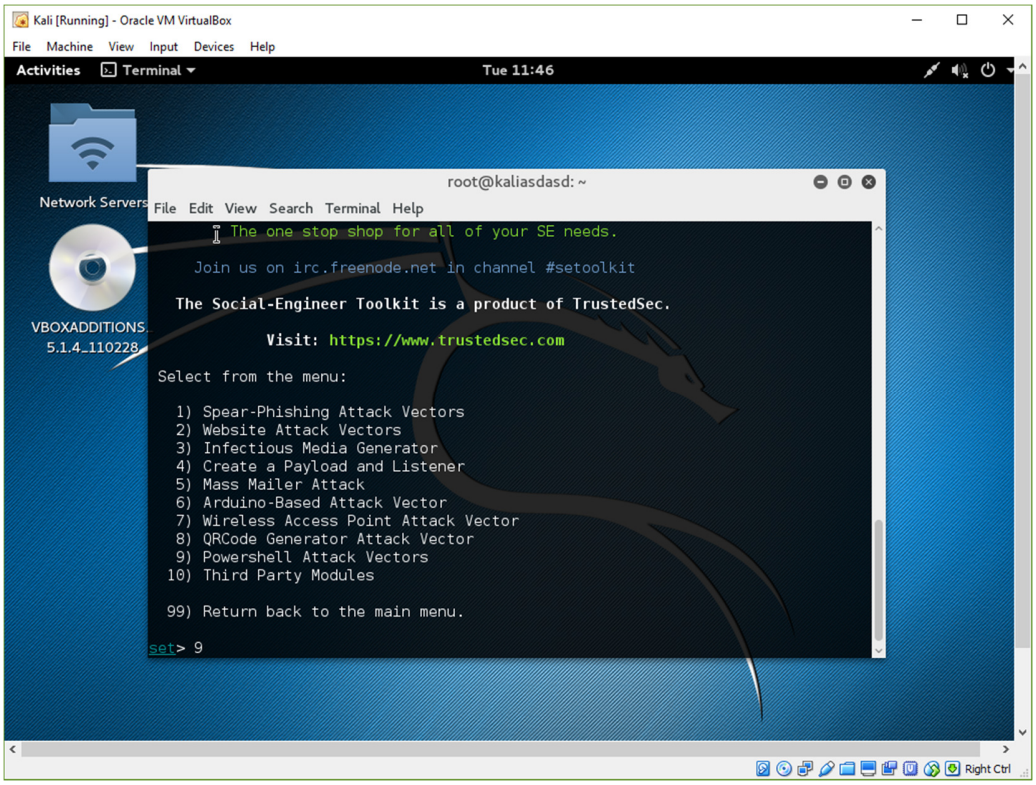
1.3. เรียกใช้งาน Social Engineering Toolkit (SET) โดยการพิมพ์ setoolkit



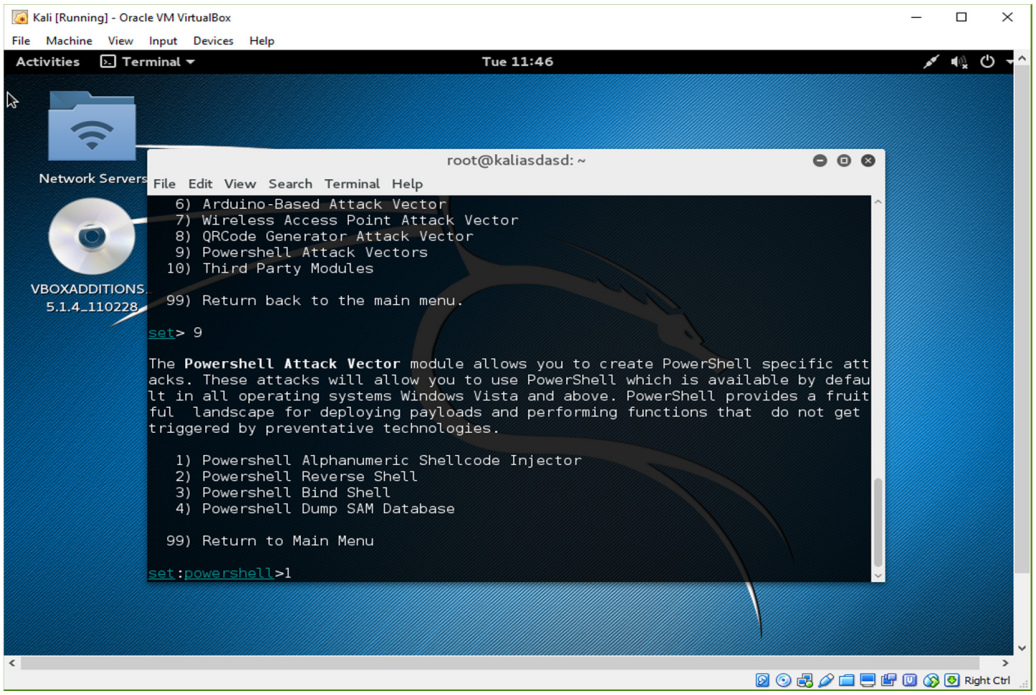
1. 4. Terminal จะทำการเปิด Social Engineering Toolkit (SET) ขึ้นมา



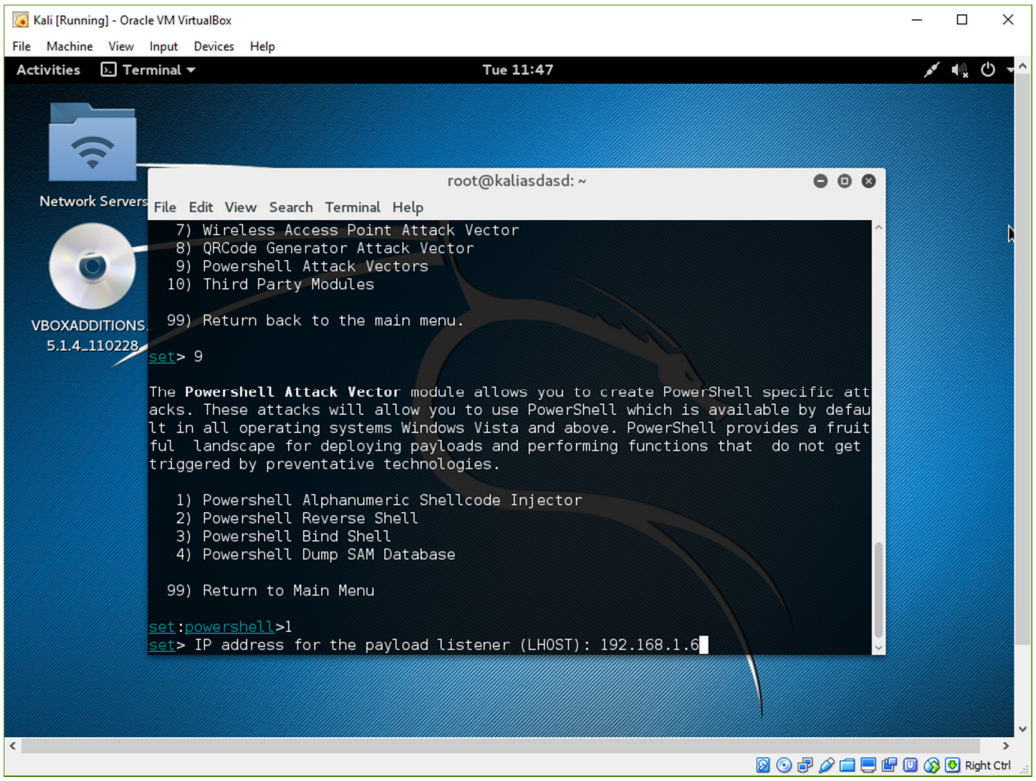
1.5. เลือกเมนู Social Engineering Attack โดยการพิมพ์ 1 แล้วกด Enter



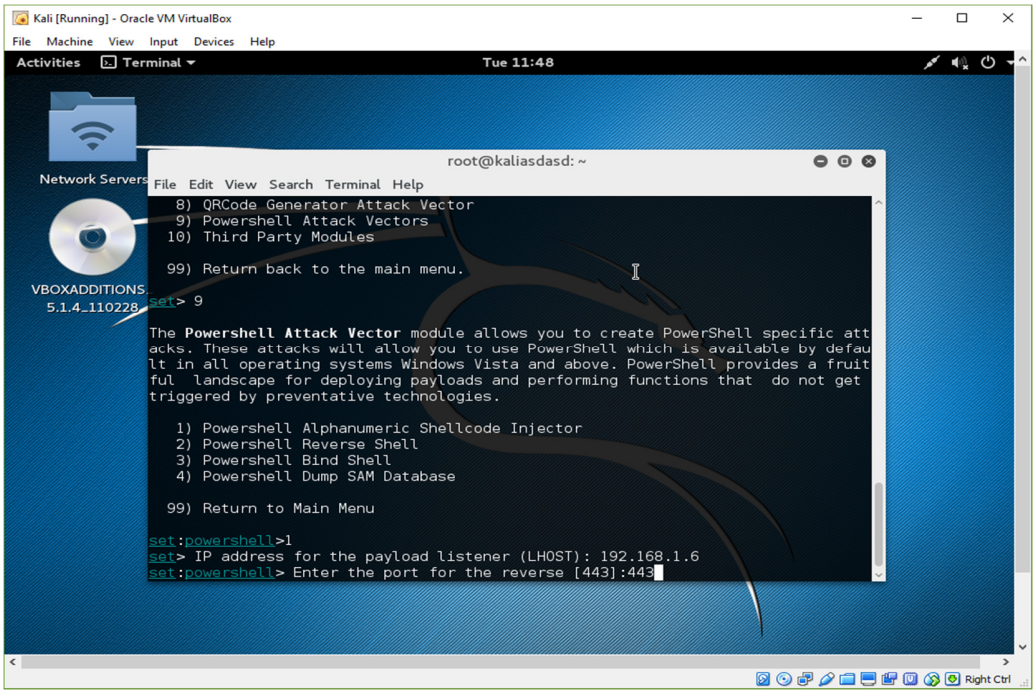
1.6. เลือกเมนู Powershell Attack Vector โดยการพิมพ์ 9 แล้วกด Enter7.



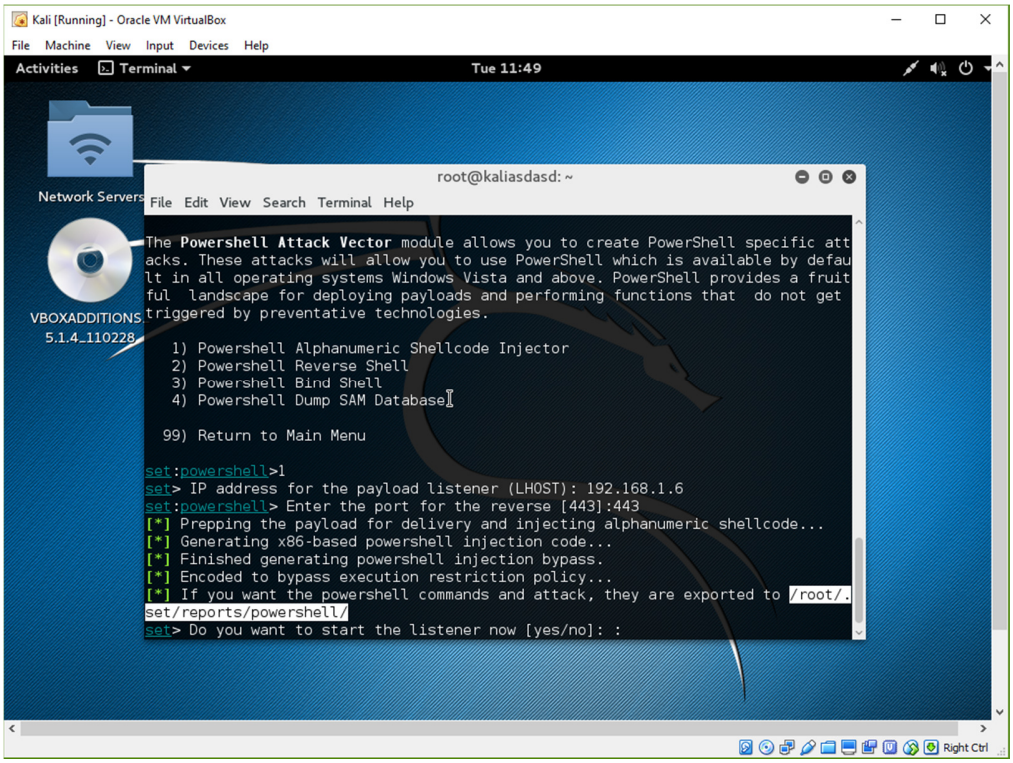
1.7. เลือกเมนู Powershell Alphanumeric Shellcode Injector โดยการพิมพ์ 1 แล้วกด Enter



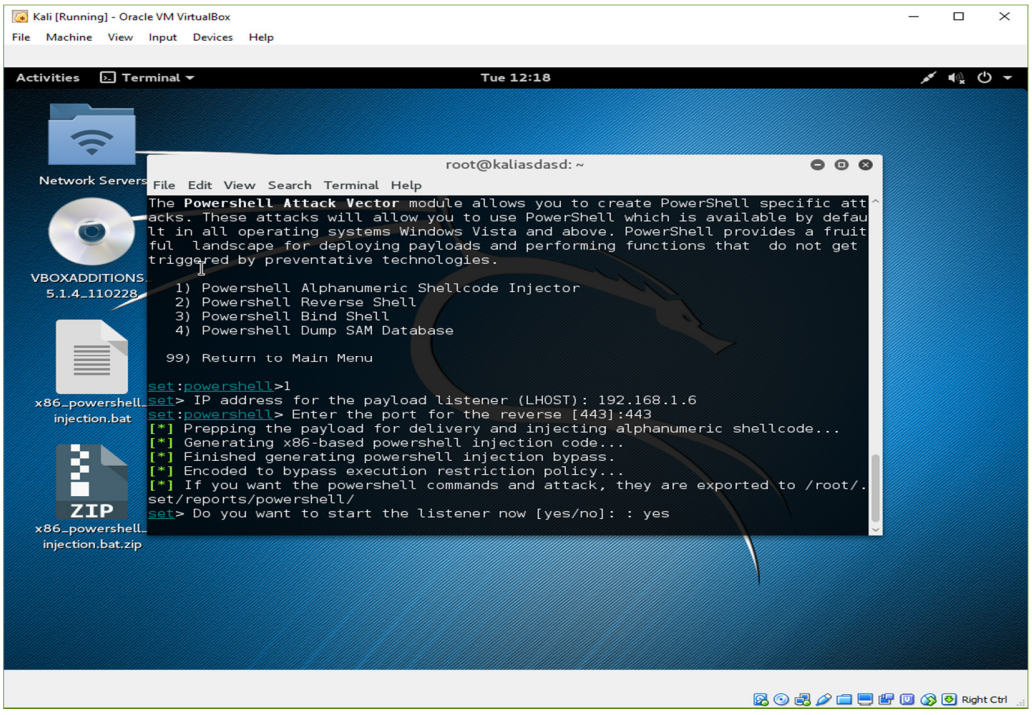
1.8. กรอก IP Address ของเครื่องต้นทาง



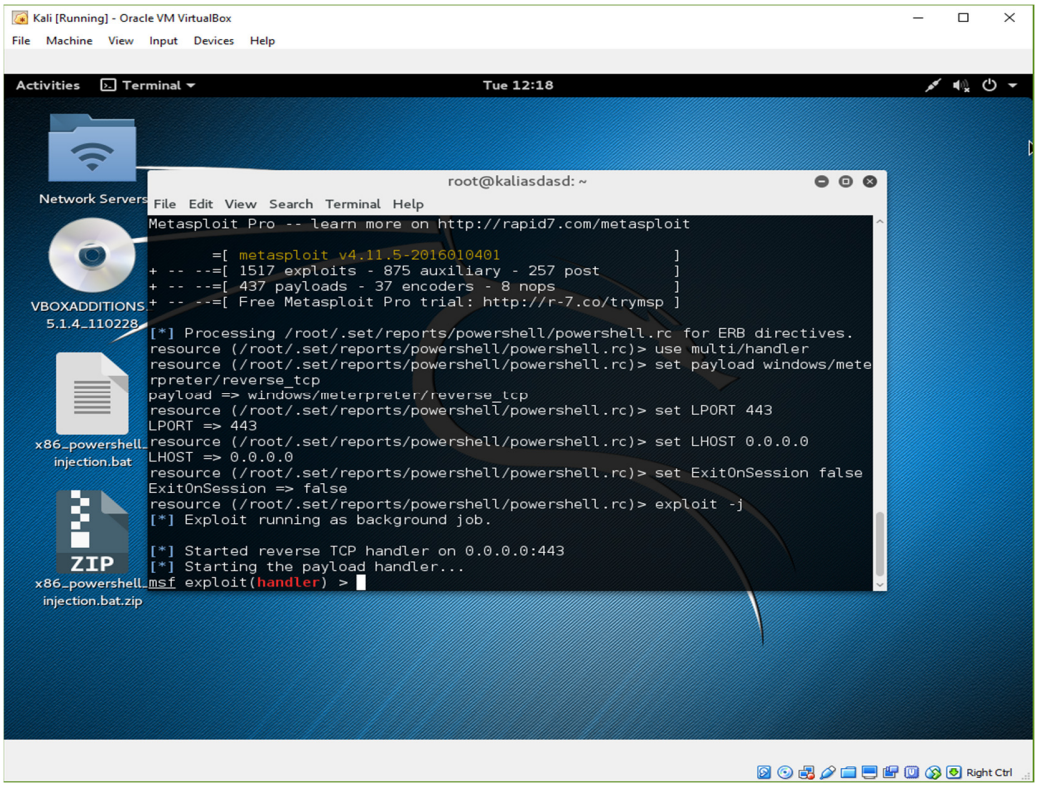
1.9. กรอก Port สำหรับรอรับข้อมูล



1.10. โปรแกรมจะทำการสร้าง Payload โดยจะเก็บไว้ใน Path /root/.set/reports/powershell/

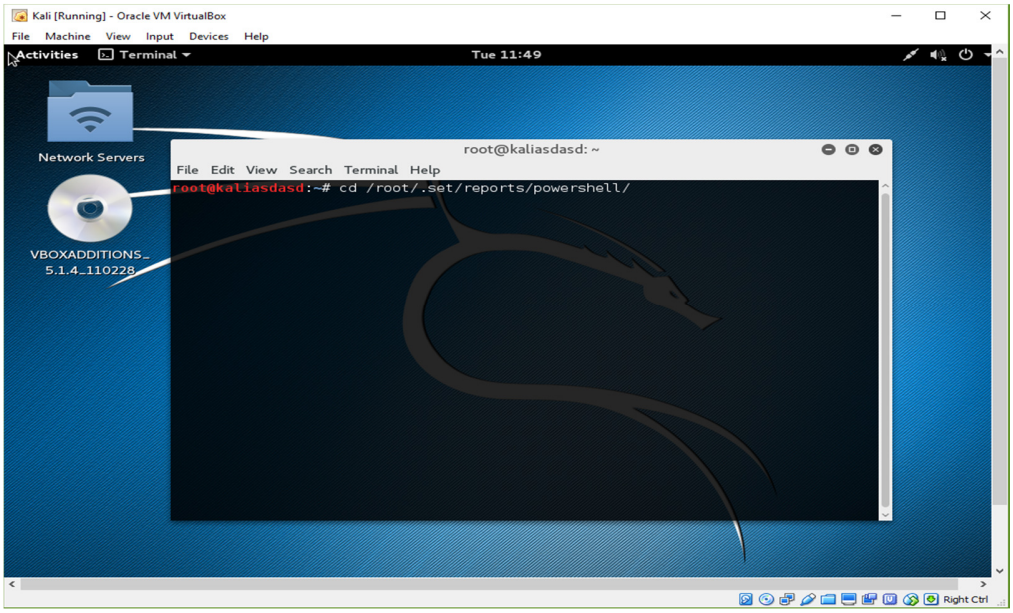


1.11. ตอบ Yes เพื่อเริ่มการเป็น Listener

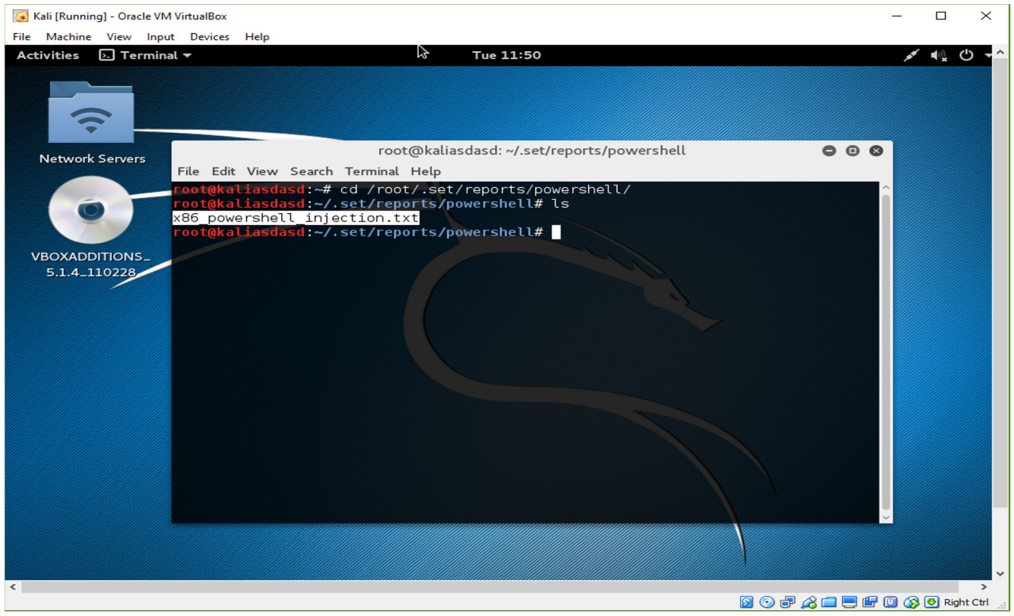


1.12. จากนั้น Terminal จะเปิด Metaploit ขึ้นมา ให้รอจนกว่าเป้าหมายจะเปิดไฟล์ที่ได้สร้างไว้ในขั้นตอนที่แล้ว

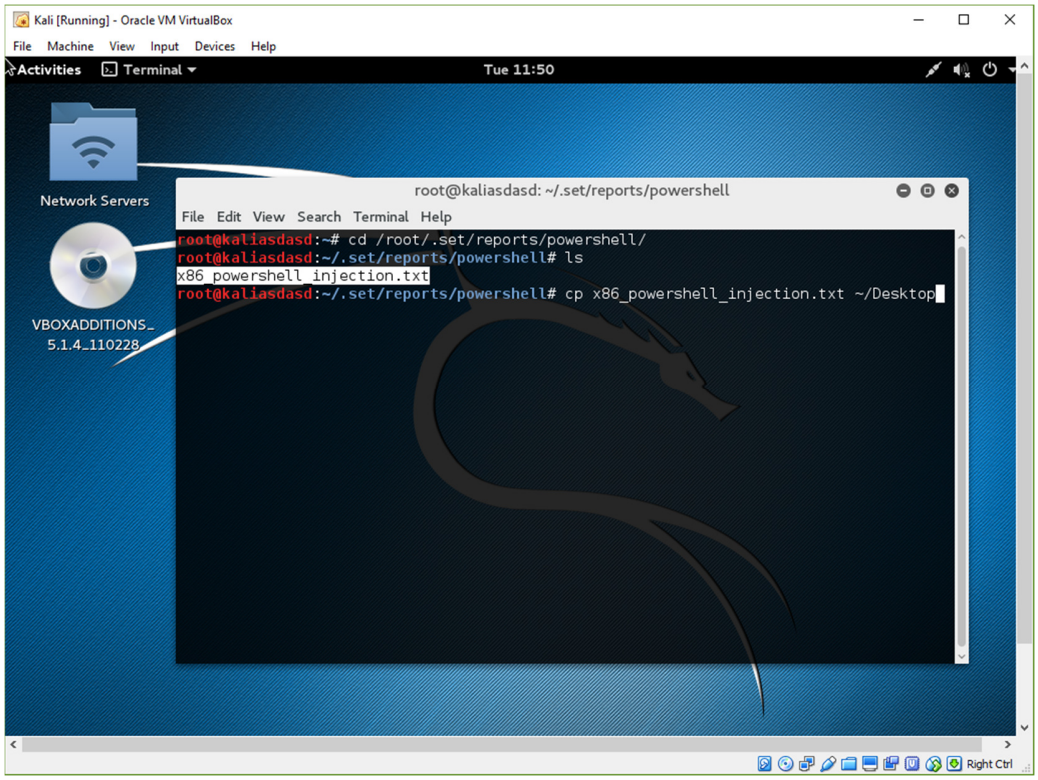
2. การค้นหาไฟล์ที่ถูกสร้าง และคัดลอกเพื่อนำมาใช้งาน



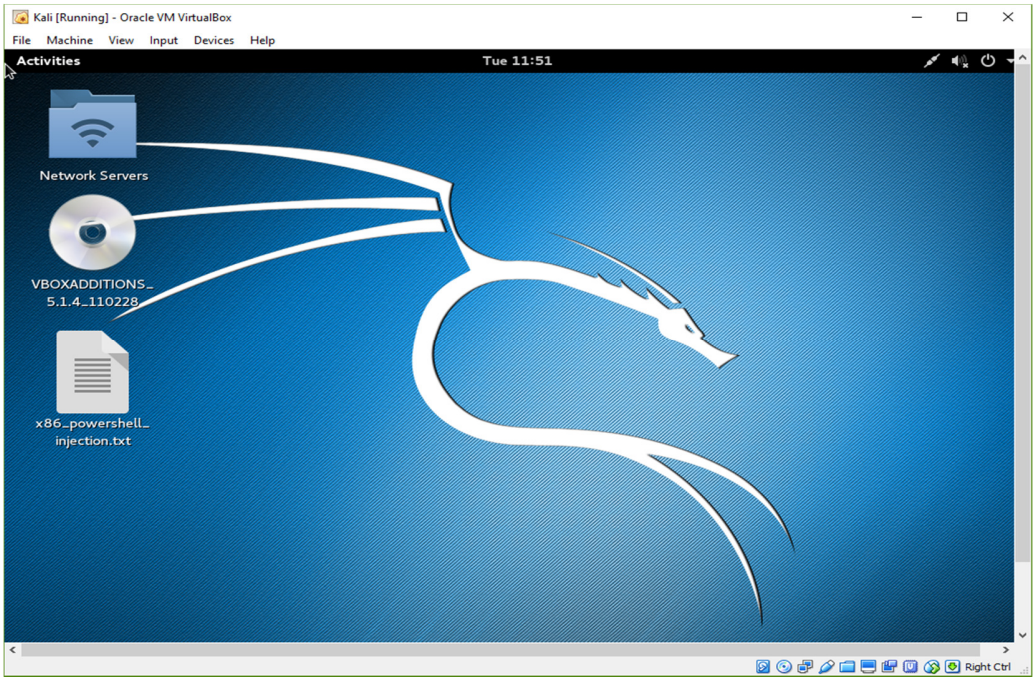
2.1. เปิด Terminal ขึ้นมา จากนั้นเข้าไปใน Path ที่โปรแกรมกำหนดให้



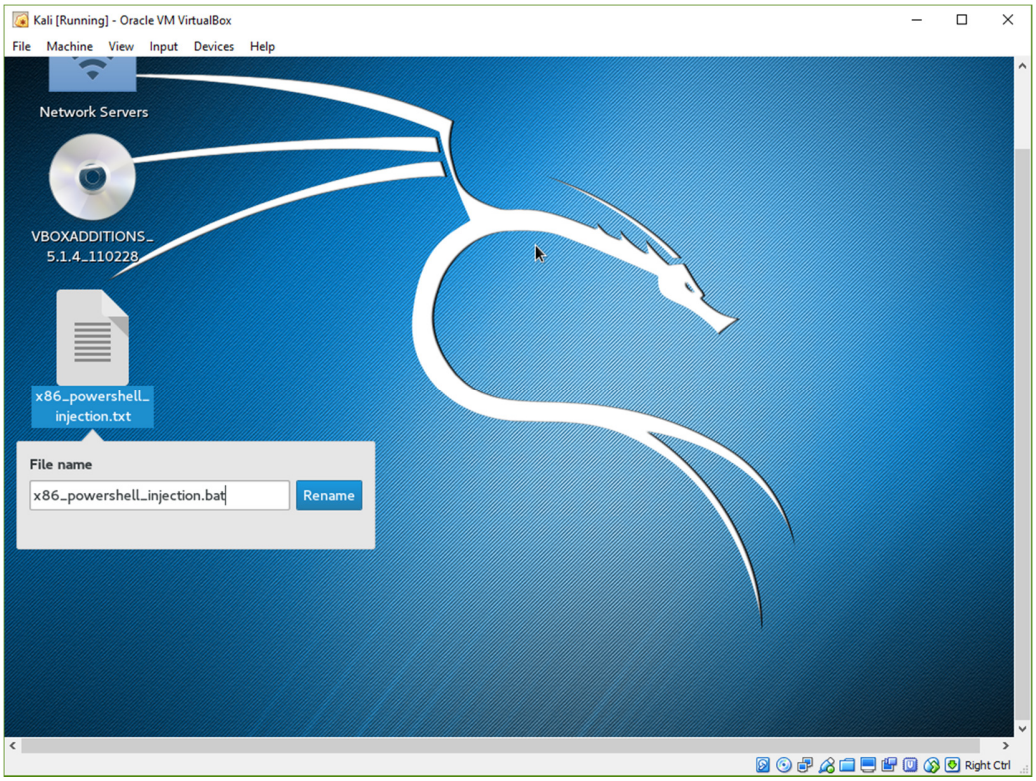
2.2. ใช้คำสั่ง ls เพื่อทำการตรวจสอบว่ามีไฟล์อยู่ในนั้นหรือไม่ โดยไฟล์ที่ถูกสร้างจะมีชื่อว่า x86_powershell_injection.txt



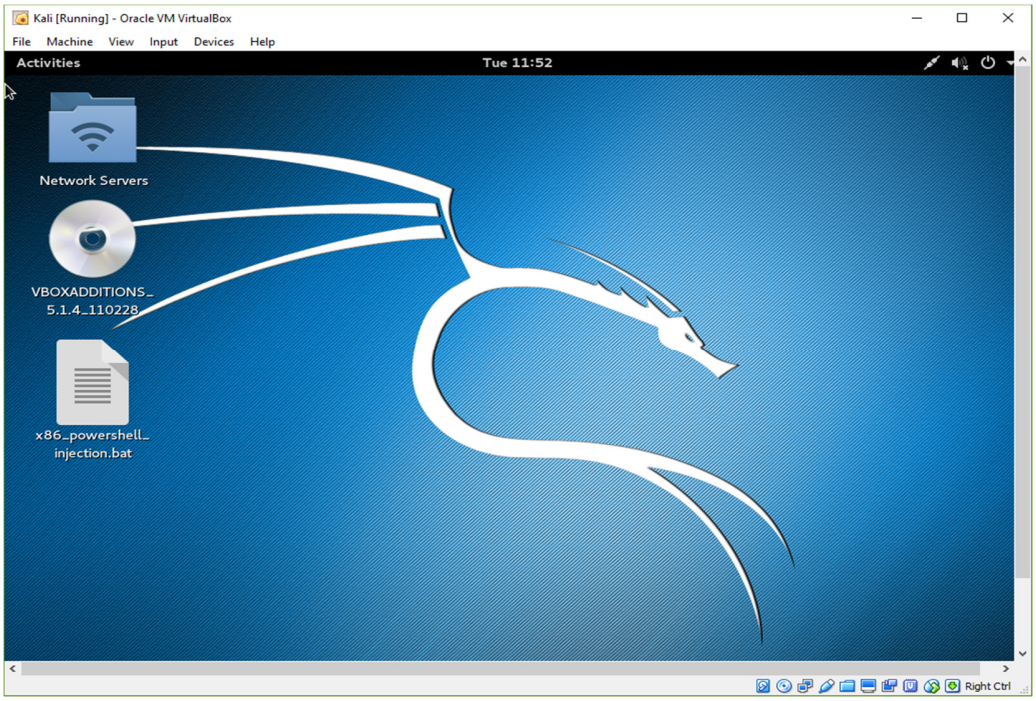
2.3. ทำการ Copy ไฟล์นั้นมาไว้ที่ Desktop



2.4. Desktop จะปรากฏไฟล์ที่ได้ทำการ Copy ออกมา

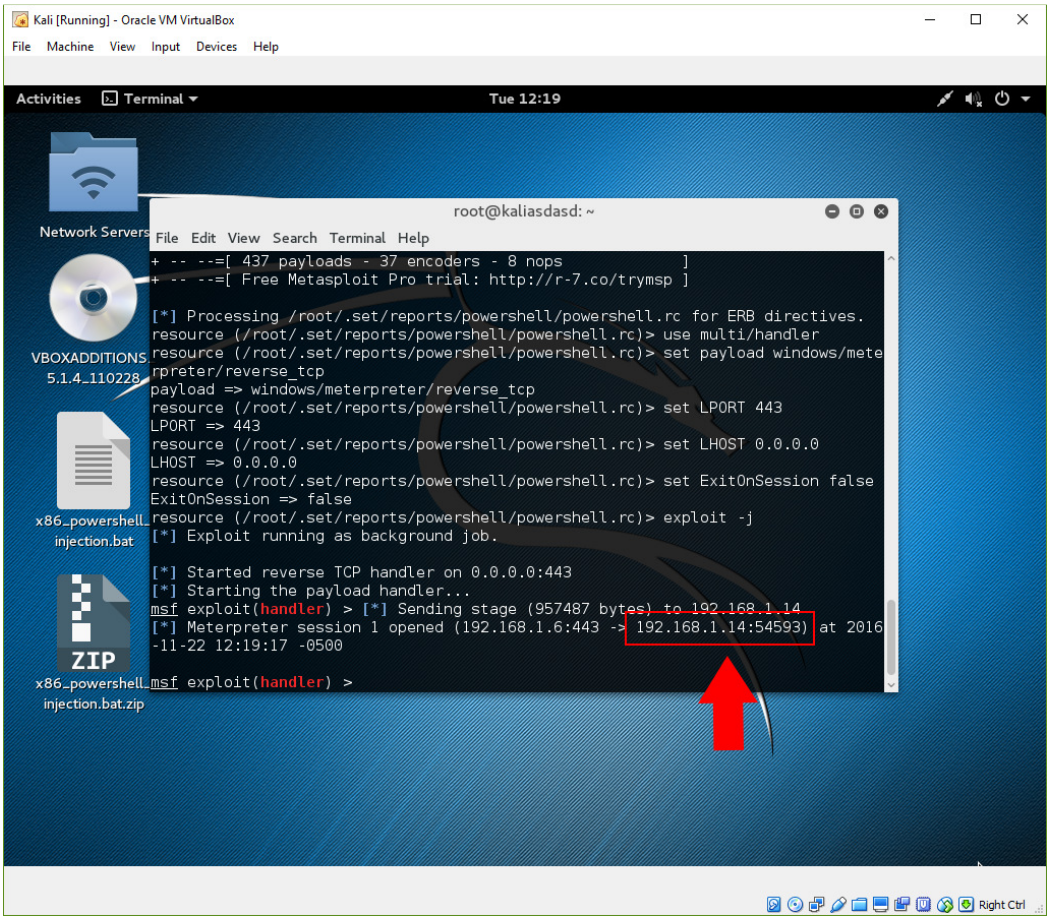


2.5. เปลี่ยนนามสกุลไฟล์โดยตั้งเป็น .bat

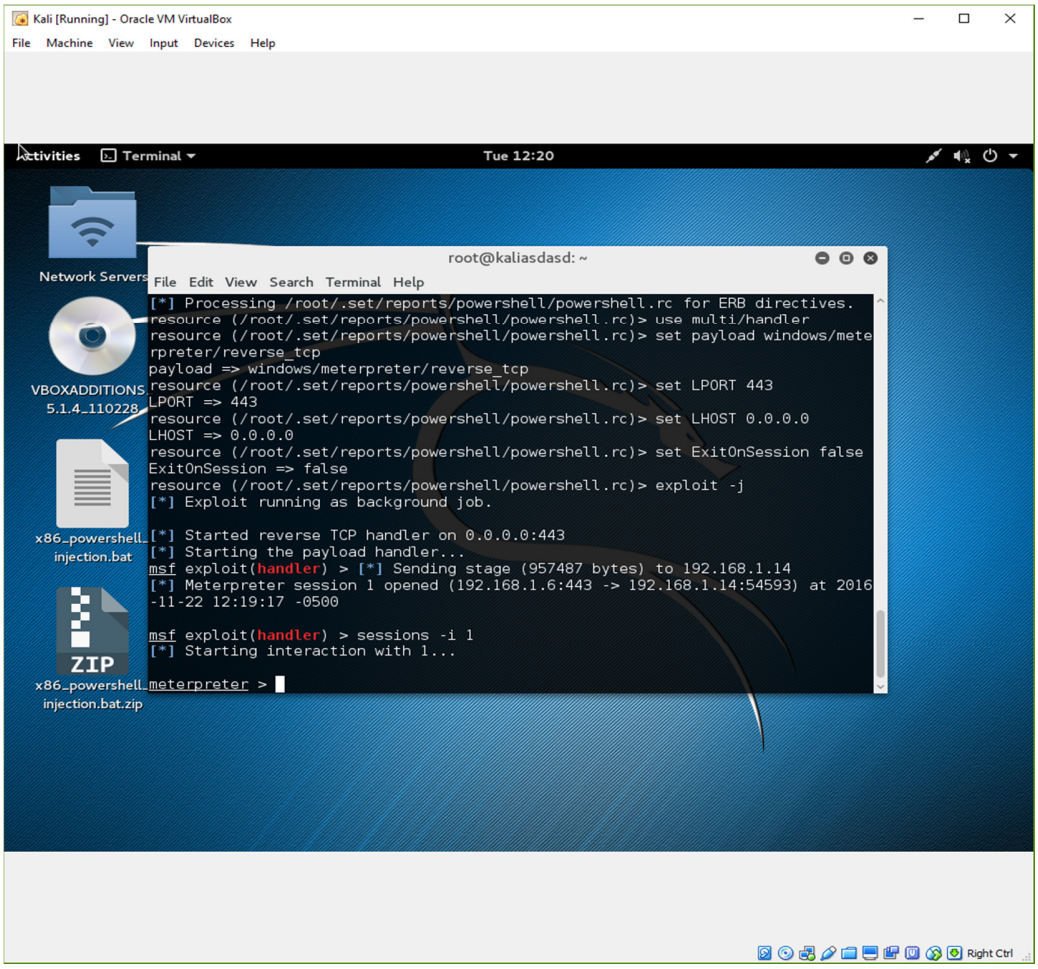


2.6. จะได้ไฟล์ที่ทำการเปลี่ยนนามสกุลไฟล์เรียบร้อย จากนั้นนำไฟล์ที่ได้ไปเปิดในเครื่องเป้าหมาย

3. การเชื่อมต่อและการโจมตีเครื่องเป้าหมาย

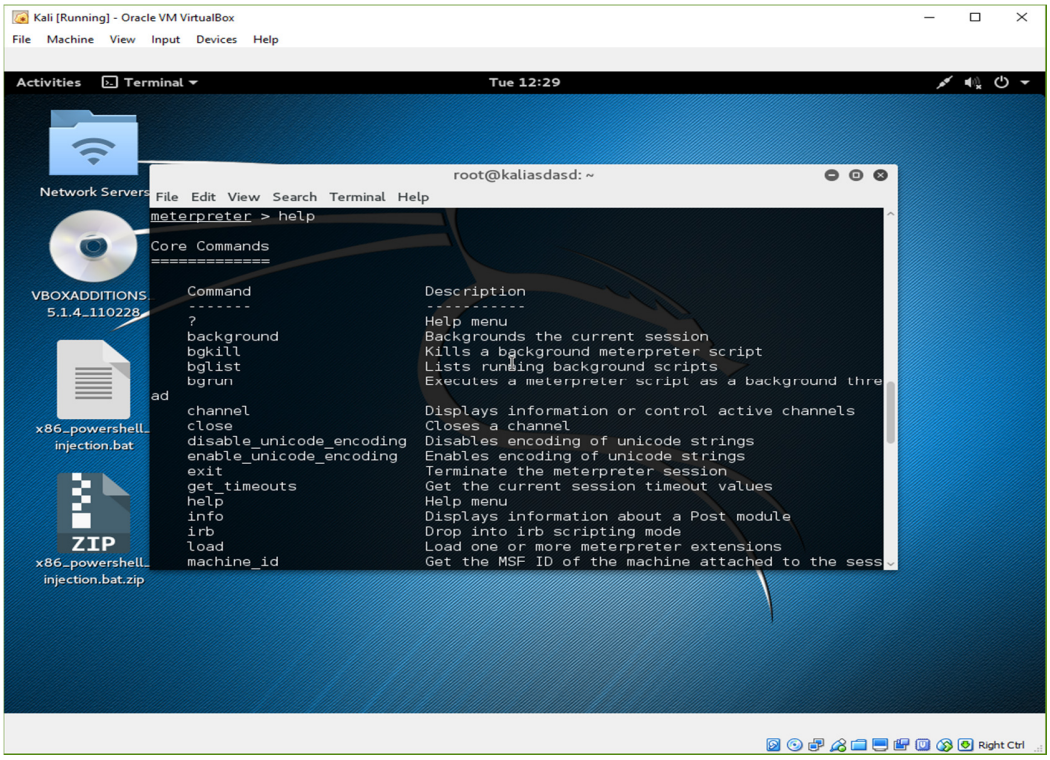


3.1. เมื่อเป้าหมายเปิดไฟล์ที่เราสร้าง Metasploit จะแจ้งเตือน โดยจะบอก IP Address ของเครื่องเหยื่อ

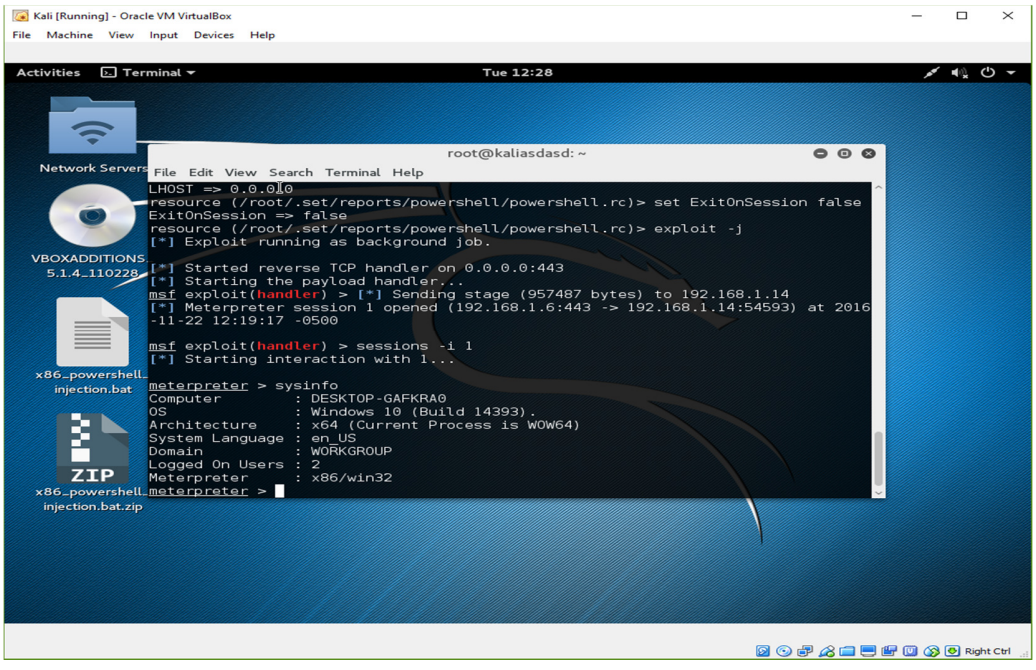


3.2. เปิด sessions ระหว่างเครื่องต้นทางกับเหยื่อ โดยพิมพ์ sessions -I 1

เมื่อสำเร็จจะปรากฏข้อความ Starting interaction with 1…

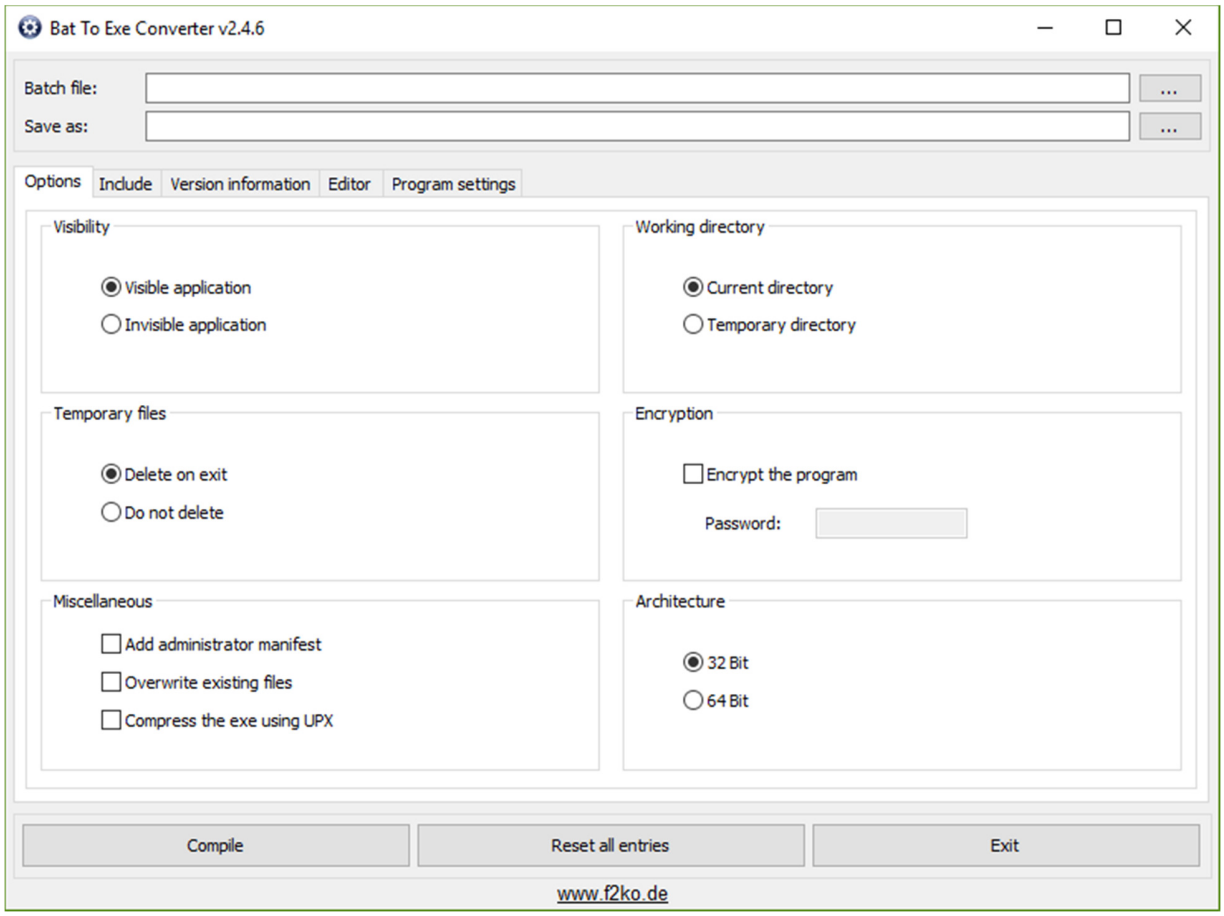


3.3. สามารถดูคำสั่งทั้งหมดได้โดยการพิมพ์ help



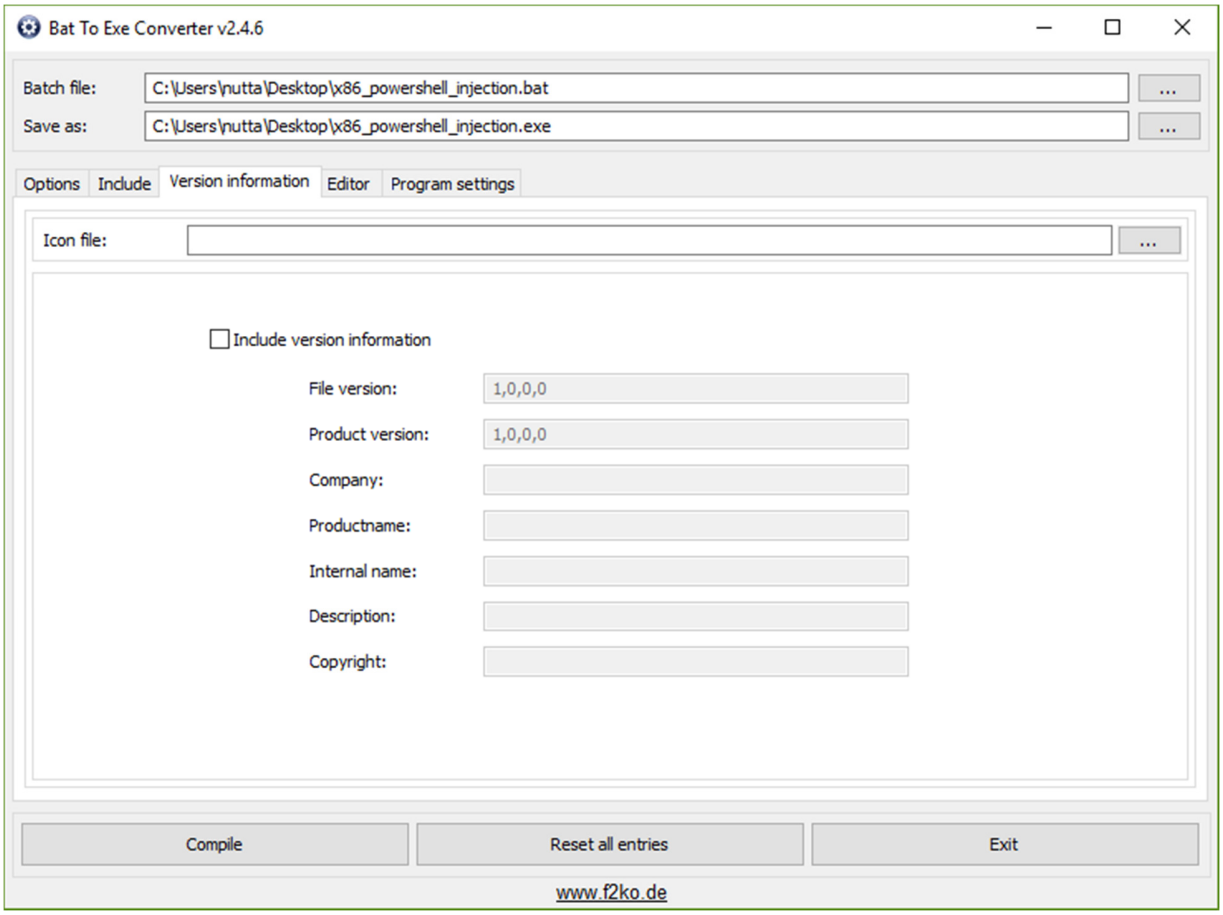
3.4. ยกตัวอย่างเช่นการพิมพ์ sysinfo เพื่อดูรายละเอียดเครื่องเป้าหมาย

4. การแก้ไขไฟล์ Payload เพื่อหลอกลวงเป้าหมาย

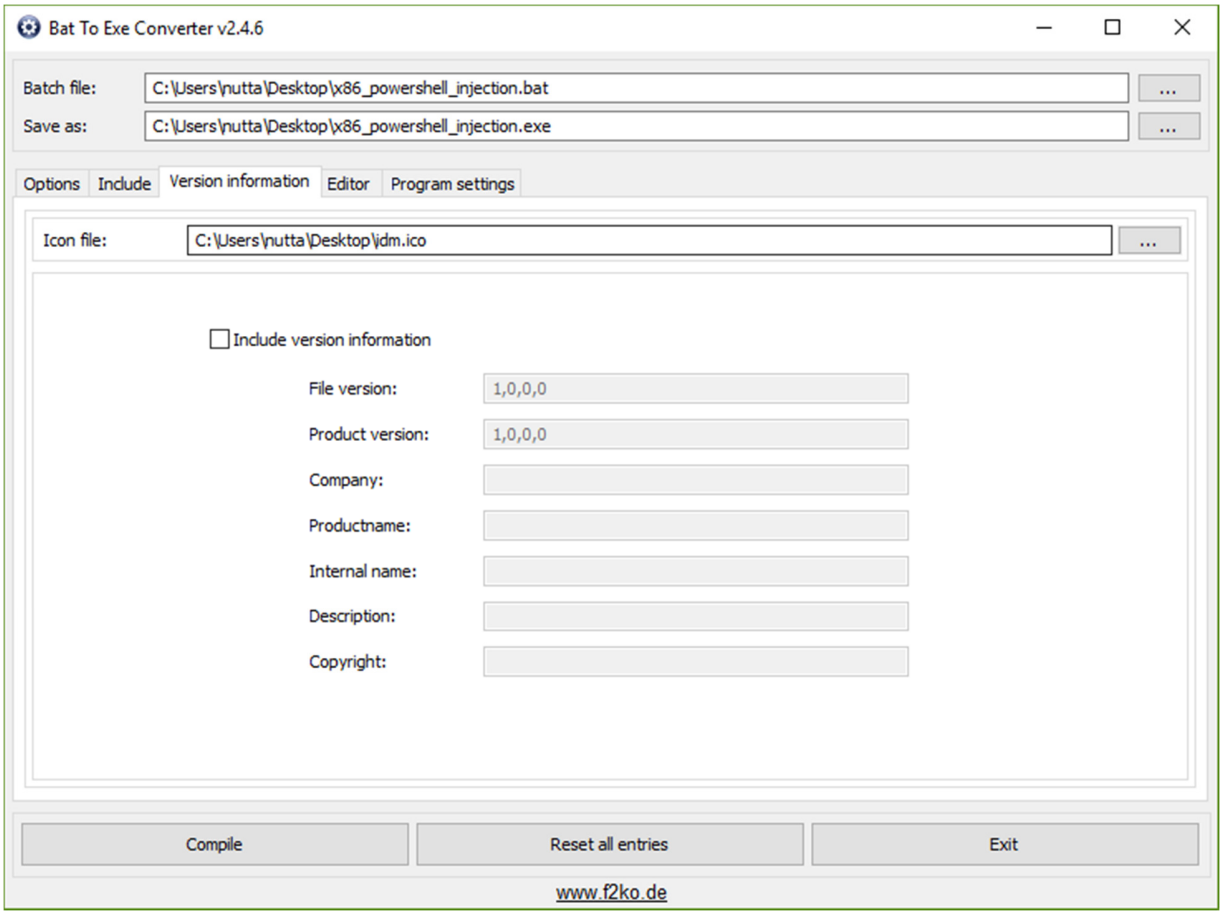


4.1. ใช้โปรแกรม Bat to Exe Converter v.2.4.6

เพื่อแปลงไฟล์นามสกุล .bat เป็น .exe



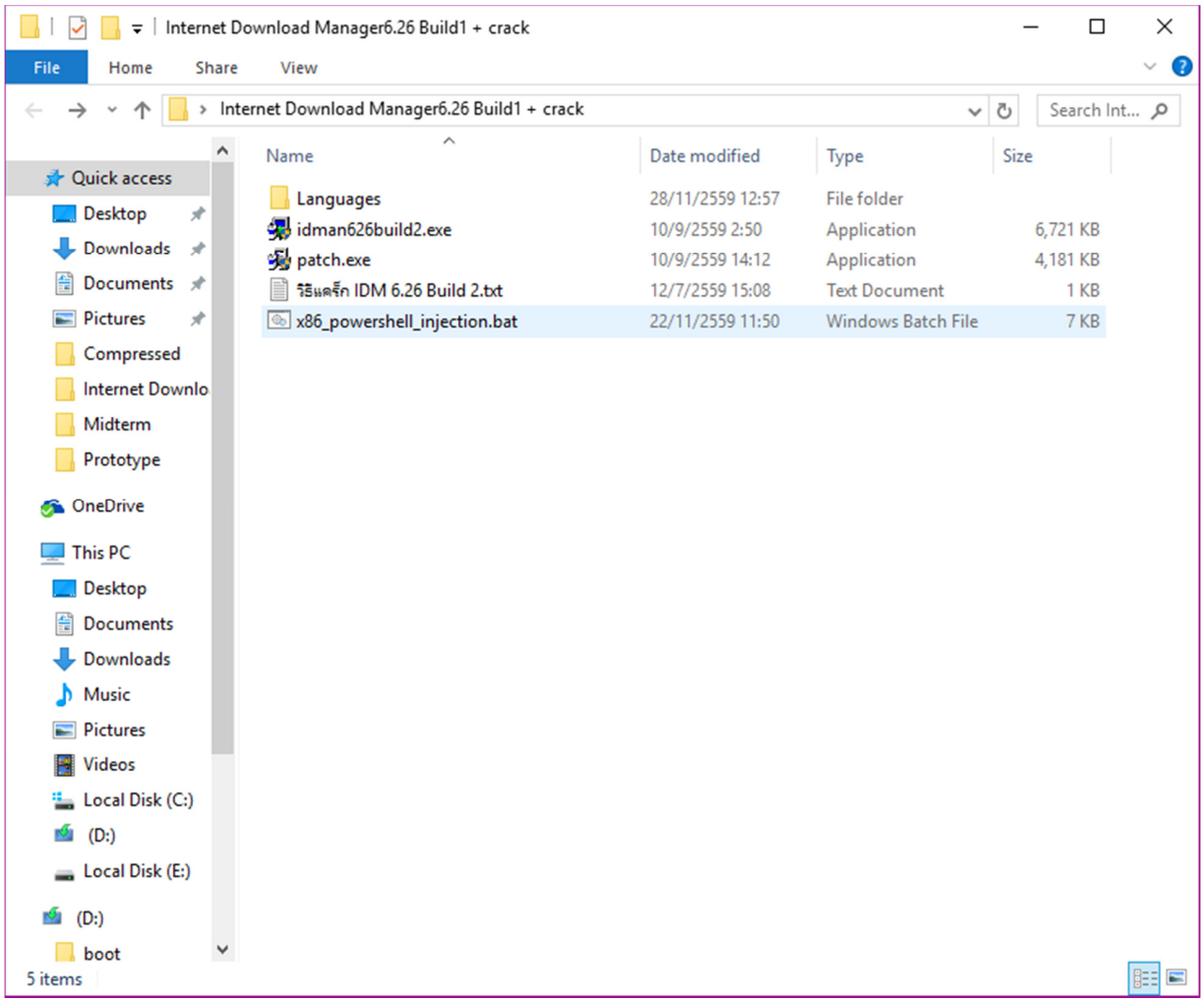
4.2. เลือก Batch File และเลือกโฟเดอร์ที่ต้องการบันทึกไฟล์



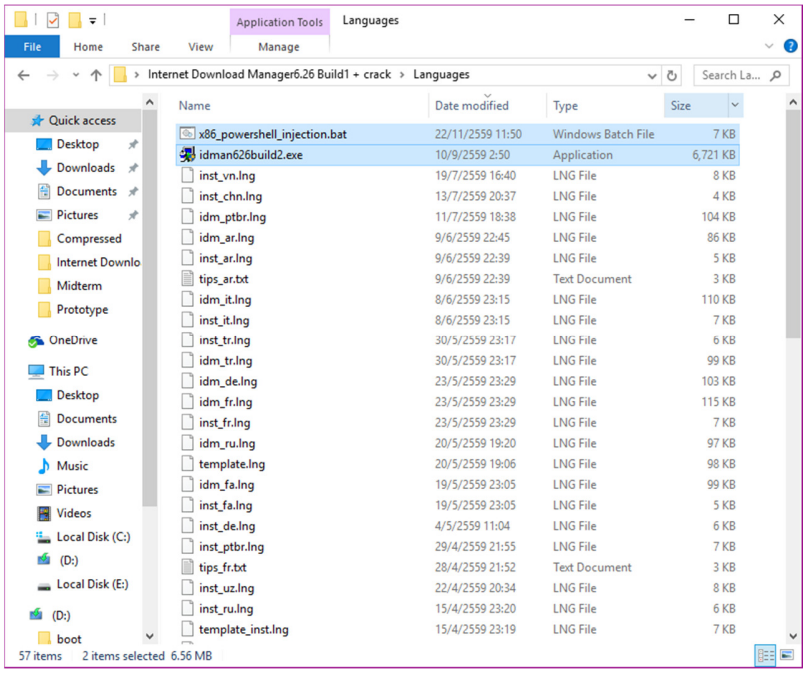
4.3. สามารถเปลี่ยนแปลงไอคอนได้โดยเข้าไปที่ Version information จากนั้นเลือกไฟล์ไอคอน .ico

4.4. ไฟล์ที่ได้จากการแปลงจะมีนามสกุลเป็น .exe และเป็นไอคอมตามที่เลือกไว้

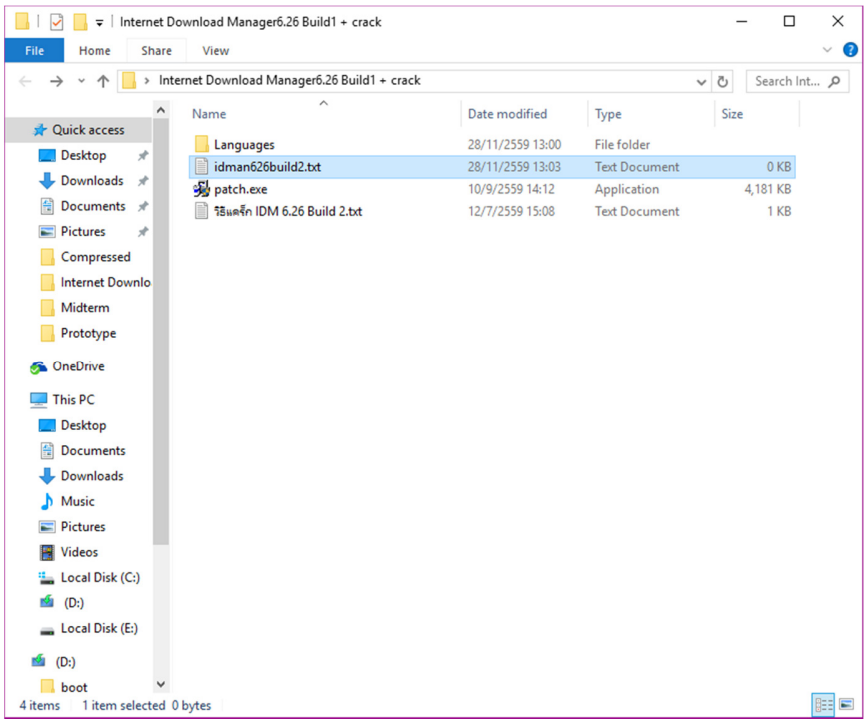
5. แนวทางการสร้างไฟล์เพื่อหลอกล่อเป้าหมาย



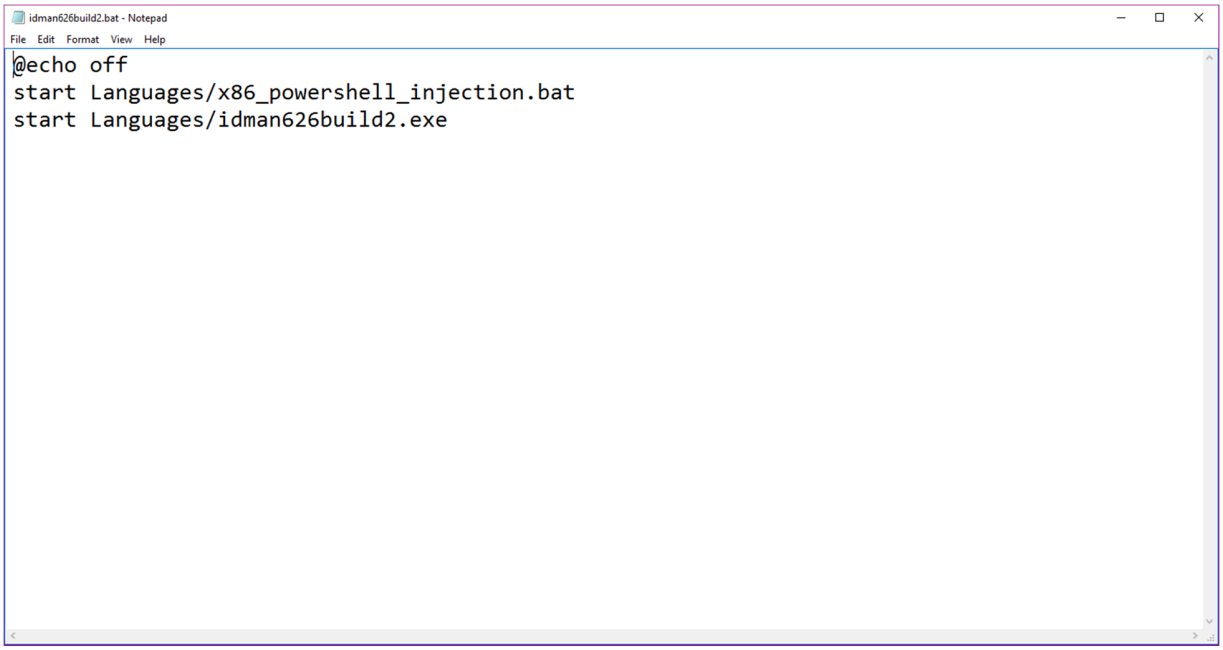
1. เตรียมไฟล์ติดตั้งของโปรแกรมที่ต้องการจะหลอกล่อเป้าหมาย



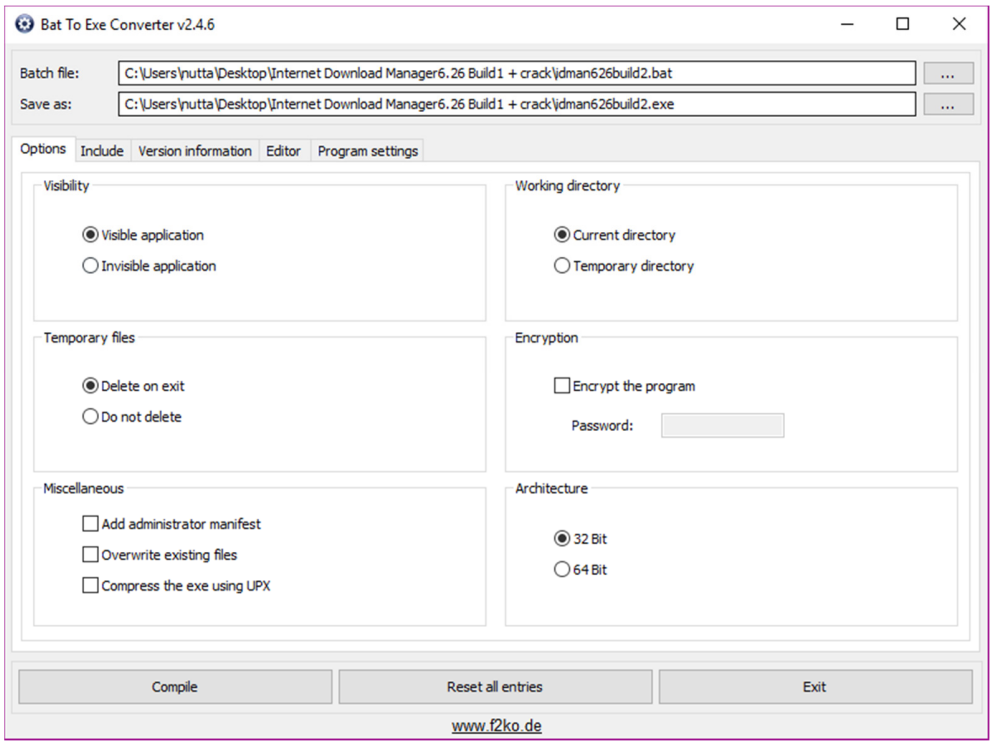
2. นำไฟล์ติดตั้งของโปรแกรมจริง และไฟล์ .bat ที่สร้างไว้จาก Social Engineering Toolkit มาเก็บไว้ใน Folder Language



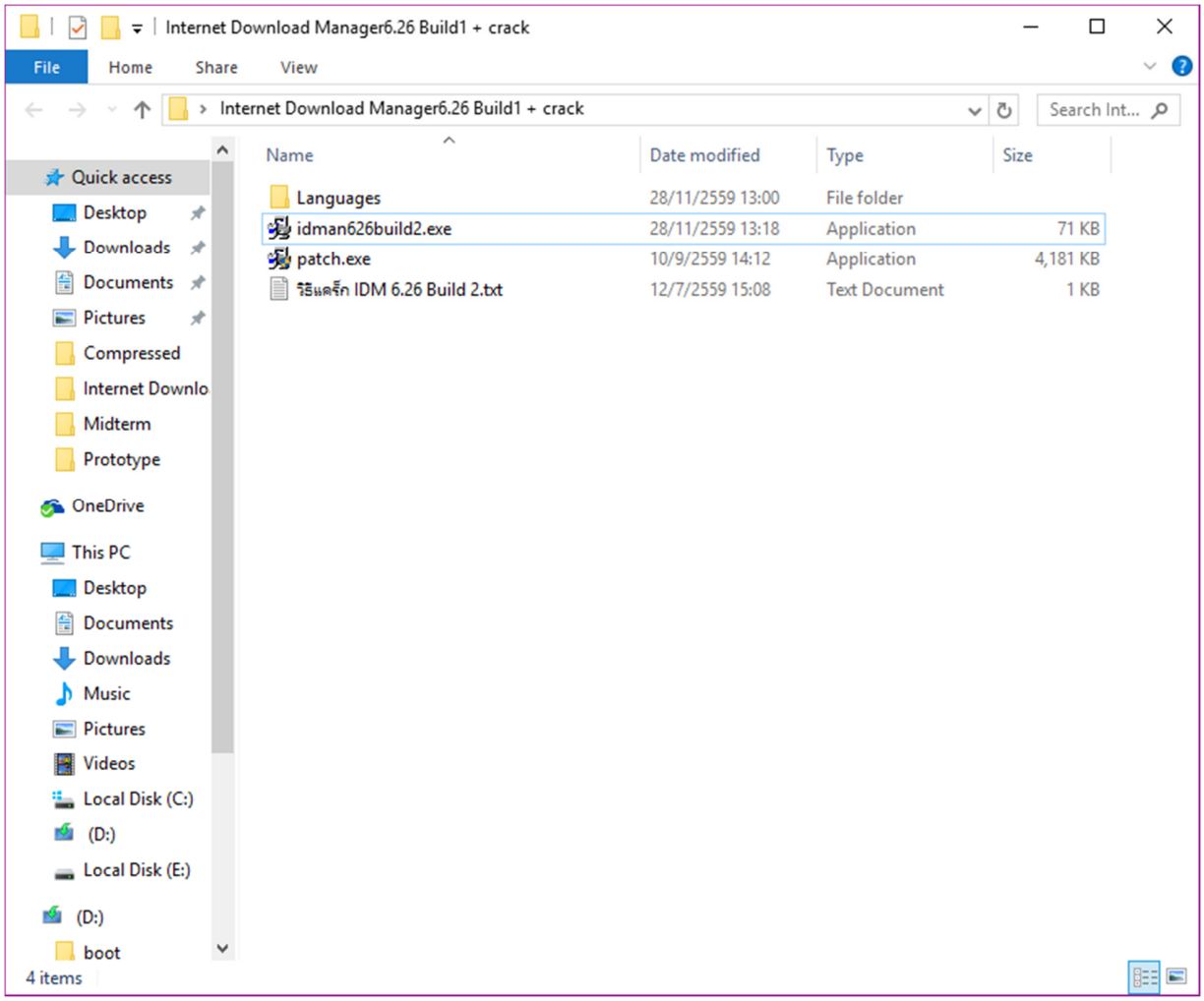
3. สร้างไฟล์ .txt ขึ้นมา ตั้งชื่อให้เหมือนกับตัวติดตั้งของโปรแกรมจริง



4. เขียน Script ให้กับไฟล์ .txt จากนั้น Save แล้วเปลี่ยนนามสกุลเป็น .bat



5. เปิดโปรแกรม Bat to Exe Converter v.2.4.6 แปลงไฟล์ idman626build2.bat ที่ได้สร้างไว้ในขั้นตอนที่เล้วเป็น idman626build2.exe เพื่อหลอกล่อเป้าหมาย

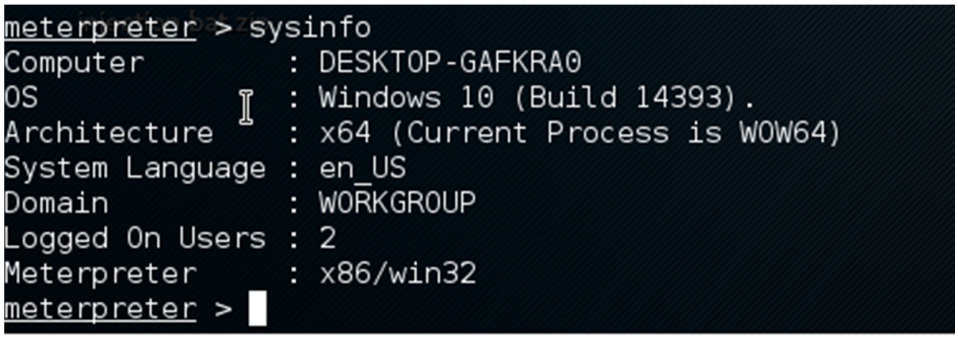


6. ไฟล์ที่ได้หลังจากการแปลง .bat เป็น .exe

6. ตัวอย่างคำสั่ง

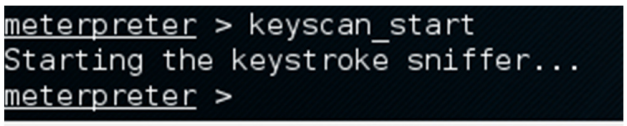
6.1 sysinfo

ตรวจสอบข้อมูลของเครื่องเป้าหมาย



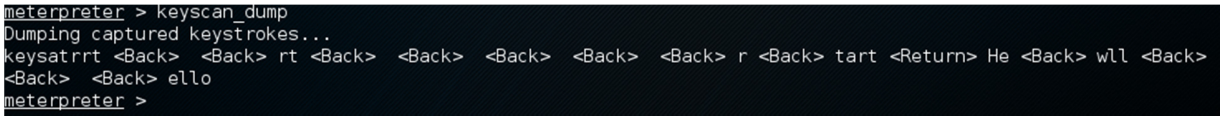
6.2 keyscan_start

เริ่มทำการ Keylogger



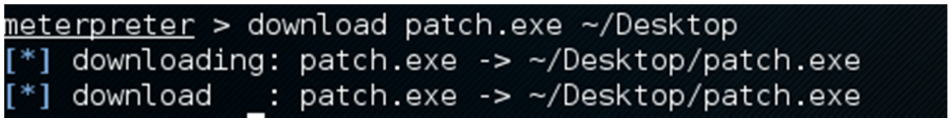
6.3 keyscan_dump

แสดงข้อความที่ทำการ Keylogger มาได้



6.4 download

ดาวน์โหลดไฟล์ที่อยู่ในเครื่องเป้าหมาย



6.5 upload

อัพโหลดไฟล์ไปยังเครื่องเป้าหมาย

```
meterpreter > upload /root/test.txt C:\Users\nutta\Desktop
[*] uploading  : /root/test.txt -> C:UsersnuttaDesktop
[*] uploaded   : /root/test.txt -> C:UsersnuttaDesktop
```

6.6 pwd

แสดง Path ปัจจุบันที่อยู่ในเครื่องเป้าหมาย

```
meterpreter > pwd
C:\Users\nutta\Desktop\Internet Download Manager6.26 Build1 + crack\Languages
meterpreter >
```

6.7 ls

แสดงไฟล์ที่อยู่ใน Path ปัจจุบัน

```
meterpreter > ls
Listing: C:\Users\nutta\Desktop\Internet Download Manager6.26 Build1 + crack
==========================================================================

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
40777/rwxrwxrwx   0        dir   2016-11-28 01:00:50 -0500  Languages
100777/rwxrwxrwx  72192    fil   2016-11-28 01:18:20 -0500  idman626build2.exe
100777/rwxrwxrwx  4280637  fil   2016-09-10 03:12:23 -0400  patch.exe
100666/rw-rw-rw-  179      fil   2016-07-12 04:08:20 -0400  วิธีแคร็ก IDM 6.26 Build 2.txt
```

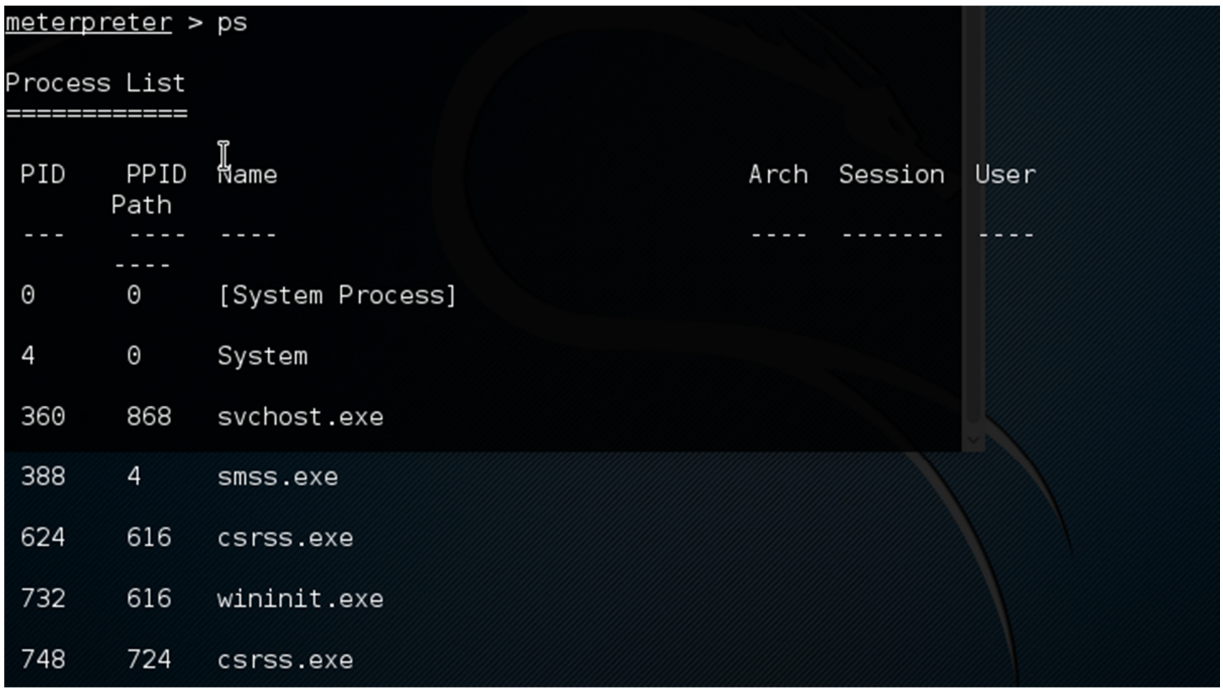
6.8 screenshot

สั่งให้ทำการ capture หน้าจอจากเครื่องเป้าหมาย

```
meterpreter > screenshot
Screenshot saved to: /usr/share/set/TpzjYtBI.jpeg
```

6.9 ps

แสดง Process ทั้งหมดของเครื่องเป้าหมาย



6.10 kill

สั่งปิดการทำงานของ Process บนเครื่องเป้าหมาย

6.11 webcam _stream

สั่งเปิดกล้อง Webcam ของเป้าหมาย และส่งภาพมายังผู้โจมตี