

การโจมตีด้วยโทรจัน(Beast) จัดทำโดย

1.นายณัฐพันธ์	กันเสนา	553020436-2
2.นางสาวนาถนภา	โต้หนองแปน	553020448-5
3.นางสาวรัตนา	มอบสันเทียะ	553020464-7
4.นางสาวอภิญญา	ไสยโสภณ	553020476-0
5.นางสาวณัฏฐณิชา	โพธิ์สว่าง	553020984-1
6.นางสาวสุธีกานต์	แต้สกุล	553021030-5

นักศึกษาระดับปริญญาตรี ชั้นปีที่ 3

หลักสูตรวิทยาการคอมพิวเตอร์ สาขาวิชาเทคโนโลยีสารสนเทศและการสื่อสาร (ภาคพิเศษ)

เสนอ

ผศ.ดร.จักรชัย โสอินทร์

ງີ້ຫາ 322376 INFORMATION AND COMMUNICATION TECHNOLOGY SECURITY

Section 4

ภาคการศึกษาที่ 1 ปีการศึกษาที่ 2557 คณะวิทยาศาสตร์ มหาวิทยาลัยขอนแก่น รายงาน ฉบับนี้ เป็นส่วนหนึ่งของวิชา 322376 INFORMATION AND COMMUNICATION TECHNOLOGY SECURITY กลุ่ม 4 ของนักศึกษาชั้นปีที่ 3 สาขา เทคโนโลยีสารสนเทศและการสื่อสาร โดยมีจุดประสงค์ เพื่อนำเสนอเนื้อหาเกี่ยวกับม้าโทรจัน ซึ่งรายงานนี้มีเนื้อหาความรู้เรื่องการโจมตี โดยการฝังม้าโทรจันไว้ที่เครื่องของฝ่ายตรงข้าม ผู้จัดทำ ได้เลือกหัวข้อนี้ในการทำรายงาน เนื่องมาจากเป็นเรื่องที่น่าสนใจ การจัดทำรายงานนำเสนอเนื้อหา ข้อมูลในครั้งนี้ เพื่อเป็นแนวทางการศึกษา ผู้จัดทำหวังว่ารายงานฉบับนี้จะให้ความรู้ และเป็น ประโยชน์แก่ผู้อ่านทุก ๆ ท่านหากมีข้อผิดพลาดประการใดต้องขออภัยมา ณ ที่นี้ด้วย

คณะผู้จัดทำ



รูปที่ 1 : ปิดโปรแกรมสแกนไวรัสภายในเครื่อง

		- • ×
COO 🗢 🔐 « All Control I	Panel Items 🔸 Windows Firewall 🕨 Customize Settings 📼 🍫 Search Control Panel	Q
Custor You can What are Home o Wallie Public n Wallie Solution	Panel Items Windows Firewall Customize Settings Image: Search Control Panel mize settings for each type of network Image: Search Control Panel modify the firewall settings for each type of network location that you use. Image: Search Control Panel modify the firewall settings for each type of network location that you use. Image: Search Control Panel Image: Image: Search Control Panel Image: Search Control Panel Image: Image: Search Control Panel Image: Search Control Panel Image: Image: Search Control Panel Image: Search Control Panel Image: Ima	
	OK Cancel	

รูปที่ 2 : ปิด windows Firewall



รูปที่ 3 : เข้าโปรแกรมแล้วกด Build Server

	🥐 Beast 2.	06		Statistics	
60	Server Set	tings		40 KB/s	
	Basic otifications StartUp	Name svchost.exe Pass Show No Injection	Listen Port 6666 SIN Port 9999 Olirect connection Reverse connection	20 KB/s	
	Misc. Exe Icon	 Inject in Internet Explore Inject in Explorer.exe Inject in notepad.exe 	r	O KB/s Bytes received: O Bytes Bytes sent: O Bytes	Duration: 00:00:0 Idle time: 00:00:0
G	Settings Save Loa	Save Server	Compress Server Hel (with built-in UPX)	Þ	
Ī	Disconnected				

รูปที่ 4 : ในแท็บ Basic เปลี่ยนจาก Direct connection เป็น Reverse connection



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



รูปที่ 6 : โปรแกรมจะแสดง IP ของเครื่องดังภาพ

Basic Notifications StartUp AV-FW Kill Misc. Exe Icon	Melt Server On Install Clear Restore Points (XP) Clear Restore Points (XP) Fake Error Mess Open Port On-Line Only No LAN notifications Delay Execution Configure	er age KB/s	
Save L	oad Save Server ♥ Compress Server (with built-in UPX) Fun Stuff Apps Server Server Services	Help KB/s Bytes received: 0 Bytes Bytes sent: 0 Bytes	Duration: 00:00:00 Idle time: 00:00:00
Disconnected	Misc Clipboard Beast Stuff Passwords		

รูปที่ 7 : ในแท็บ Misc. กำหนดข้อความแสดงข้อผิดพลาดแจ้งเครื่องเป้าหมาย

Basic Notifications	Enable KeyLogger		
🖗 Fake Error Message	- De pe	KB/s	
Message Box Icon			
2 1 8		KB/s	
Message Boy Buttons			
O DK O Yes, No, Cancel	Test H	elp KD /a	
O DK, Cancel O Retry, Cancel	ОК	Bytes received: 0 Bytes	Duration: 00:00:00
Yes, No O Abort, Retry, Ignore		Bytes sent: 0 Bytes	Idle time: 00:00:00
Message Box Title Warning			
Message Box Text This application has failed to	start because		
Use "I character for starting a new line in Message Bo	ox Text.		

รูปที่ 8 : เลือกไอคอนและข้อความแสดงผลแล้วกด OK

1	😯 Server Settings			
Port 9999	Basic Melt Server On Install Enable KeyLogg Notifications Configure StartUp Clear Restore Points (XP) AV-FW Kill Open Port On-Line Only Misc. No LAN notifications Exe Icon No LAN notifications	er ige		
	Settings Save Load Save Compress Server (with built-in UPX) Misc Clipboard Clipboard	Help	ved: O Bytes O Bytes	Duration: 00:00:00 Idle time: 00:00:00
Discor	nected			

รูปที่ 9 : เลือกเครื่องหมายถูก Fake Error Message เพื่อเปิดใช้งานการตั้งค่า

Server Setting	gs	40 KB/s	
Basic Notifications StartUp	Server Icon Choose Icon 🚔	20 KB/s	
AV-FW Kill Misc. Exe Icon		Bytes sent: 0 Bytes	0 Bytes Duration: 00:00:00 vtes Idle time: 00:00:00
Settings Save Load	Save Server Compress Server (with built-in UPX)	Help	
Disconnected	•••		

รูปที่ 10 : Exe Icon เลือกไอคอนที่จะนำไปวางในเครื่องเป้าหมาย

6 Beact 2 06		Statistics	
Server Settings		40 KB/s	
Basic Notifications StartUp AV-FW Kill Misc. Exe Icon	Choose Icon 🚔	20 KB/s 0 KB/s Bytes received: 0 Bytes Bytes sent: 0 Bytes	Duration: 00:00:00 Idle time: 00:00:00
Settings Save Load Server	(with built-in UPX)		
Disconnected			
	*		

รูปที่ 11 : กดเลือก Save Server

Peast 2.06 Statutes Server Settings 40 KB/s Basic 20 KB/s
AV-7 M M M M M Exe 0 KB/s VOK Bytes received: 0 Bytes Duration: 00:00:00 Idle time: 00:00:00
Save Load Server (with built-in UPX) Help Disconnected
serven.exe

รูปที่ 12 : โปรแกรมแสดงข้อความแจ้งว่า ทำการสร้างไฟล์ .exe ไว้เรียบร้อยแล้ว



รูปที่ 13 : นำไฟล์ .exe ที่สร้างไว้ไปเปิดในเครื่องเป้าหมาย โดยที่เครื่องเป้าหมายต้องปิด Windows Firewall และโปรแกรมสแกนไวรัส



รูปที่ 14 : ดับเบิ้ลคลิกที่ไฟล์ .exe จากนั้นระบบจะแจ้งเตือนข้อความ(ที่เครื่องโฮสตั้งค่าไว้)



รูปที่ 15 : สังเกตไฟล์ .exe ที่ลงไว้ในเครื่องเป้าหมายจะหายไป



รูปที่ 16 : ในส่วนของเครื่องที่ใช้โจมตีเป้าหมาย กด Start Listening [SIN] รอสักครู่



รูปที่ 17 : ระบบจะแสดงชื่อเครื่องที่เครื่องเป้าหมายที่ถูกโทรจันฝังไว้



รูปที่ 18 : ทางขวาของโปรแกรม สามารถเลือกพังก์ชันการใช้งานต่าง ๆ ได้ เช่น การเปิดกล้อง, เปิดถาดซีดี, สถานะการประมวลผลของระบบ, ไฟล์ในไดเรกทอรี่ต่างๆ ฯลฯ



รูปที่ 19 : ในส่วนของการเปิดกล้อง โปรแกรมจะแสดงหน้าต่างสำหรับเปิดกล้องของเครื่องเป้าหมายขึ้นมา



รูปที่ 20 : เมื่อกด Start โปรแกรมจะเปิดกล้องของเครื่องเป้าหมาย ดังภาพ



รูปที่ 21 : ในส่วนของการแชท โปรแกรมจะแสดงหน้าต่างขึ้นมาดังภาพ



รูปที่ 22 : ในส่วนของเครื่องเป้าหมาย หากผู้โจมตีส่งข้อความมาถึงเครื่องเป้าหมาย จะแสดงกล่องข้อความขึ้นมา บนหน้าจอ และสามารถตอบข้อความกลับไปได้

		0				1	
Let'sRock	EPSON Scan Ea	eye 📀 Cha	at				
e Beast Host 127.0.0.1 Password Port 9999	2.06 Port 6666 Discon Stop Listening [Sl	<beast <sucket< th=""><th>: Master> r> Hi</th><th>Hello</th><th></th><th></th><th></th></sucket<></beast 	: Master> r> Hi	Hello			
Connected			Your Nick <beast ma<br="">Victim's Nic <sucker></sucker></beast>	ster>	Close I Size 50 % of victim	Chat s screen	Send

รูปที่ 23 : ในมุมมองของเครื่องผู้โจมตี จะสามารถกำหนดชื่อผู้ส่งได้