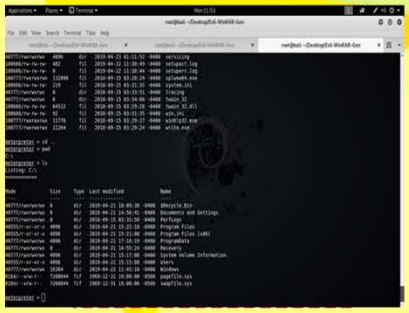
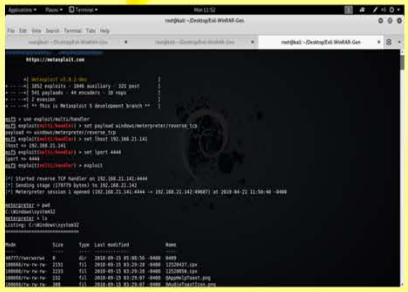
การพัฒนาการโจมตี Windows ด้วยช่องโหว่ Path Traversal

หลักการและเหตุผล

เมื่อไม่นานมานี้ ทาง The Hacker Newsรายงานข่าวการพบช่องโหว่บนโปรแกรมบีบอัดไฟล์ยอดนิยมอย่าง WinRAR ที่มีผู้ใช้ทั่วโลกมาถึง 500 ล้านราย ซึ่งเปิดโอกาสให้แฮ็กเกอร์สามารถสั่งรันโค้ดบนเครื่องเหยื่อจากระยะไกลได้ และกระทบกับ WinRAR ทุกเวอร์ชั่นตั้งแต่ที่เปิดตัวเมื่อ 19 ปีที่แล้ว นั่นคือ ถ้าแฮ็กเกอร์สร้างไฟล์อันตรายที่บีบอัดในรูปแบบของ ACE แต่หลอกเราด้วยการแก้ไขสกุลไฟล์เป็น .rar เป็นต้น ก็สามารถลอบเข้ามาใช้ไลบรารีดังกล่าวสร้างความเสียหายบนเครื่องโดยไม่ทันตั้งตัวได้ ยิ่งกว่านั้น ช่องโหว่นี้ยังบังคับให้ขยายแตกไฟล์ไปยังโฟลเดอร์ที่แฮ็กเกอร์ตั้งค่าไว้แทนตำแหน่งโฟลเดอร์ที่ผู้ใช้เลือกได้ด้วย





วัตถุประสงค์

1. เพื่อต้องการศึกษากระบวนการและวิธีการในการเจาะระบบ การโจมตีระบบ
2. เพื่อนำความรู้ที่ได้ในรายวิชา 342376 ความมั่นคงเทคโนโลยีสารสนเทศและการสื่อสารไปต่อยอดและพัฒนาต่อไป
3. เพื่อให้ได้รับประสบการณ์ที่สามารถนำไปใช้และแก้ไขสถานการณ์ในชีวิตประจำวันได้

ขอบเขตและเป้าหมายของโครงงาน

1. สามารถเข้าถึงไลบรารีของเครื่องเป้าหมายได้โดยที่เป้าหมายไม่รู้ตัว
2. ถ้าหากทาง WinRAR ทำการแก้ไขช่องโหว่แล้ว จะไม่สามารถรันได้
3. ไม่สามรถทำการแฮ็กต่อได้ถ้าเครื่องปลายทางหยุดการใช้อินเตอร์เน็ตกลางคัน

ประโยชน์ที่คาดว่าจะได้รับ

1. ได้รู้หลักการการทำงาน การพัฒนาการโจมตี Windows ด้วยช่องโหว่ Path Traversal
2. ได้เรียนรู้วิธีการเจาะระบบด้วยระบบปฏิบัติการ Kali Linux
3. ได้ทราบถึงการเข้าถึงช่องโหว่ในโปรแกรมบีบอัดไฟล์ .rar

จัดทำโดย

นางสาวกุลธิดา	เดชดี	603020335-3
นางสาวกัลยรัตน์	กำแซง	603021038-4
นายอดิสรณ์	หิรัญชา	603021064-3
นางงสาวจุฑามาส	จินจิว	603021720-5
นายพีรณัฐ	เกษกี	603021732-8
นางสาวอนุชิตา	จำปา	603021735-2

กลุ่ม 13 SECTION 2

ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยขอนแก่น