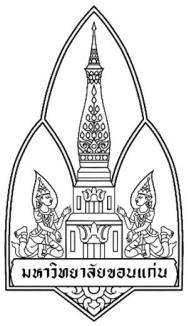


การทดสอบความปลอดภัยบนเครือข่ายไร้สาย

จัดทำโดย

1. นายทศพร ไชยชมภู	**รหัสนักศึกษา 583020160-0**
2. นางสาวจุฑาทิพย์ ฐานวิสัย	**รหัสนักศึกษา 583020651-1**
3. นางสาวศุภสุดา เรืองตระกูล	**รหัสนักศึกษา 583020683-8**
4. นายเอกราช ศรีอาภรณ์	**รหัสนักศึกษา 583021405-1**
5. นายกันตพัฒน์ ทิพย์พิมลธนา	**รหัสนักศึกษา 583021365-7**
6. นายธนพล ศรีโยธี	**รหัสนักศึกษา 583020661-8**

นักศึกษาระดับปริญญาตรี ชั้นปีที่ 2
สาขาวิชาเทคโนโลยีสารสนเทศและการสื่อสาร โครงการพิเศษ

อาจารย์ที่ปรึกษา
รศ.ดร.จักรชัย โสอินทร์

รายงานนี้เป็นส่วนหนึ่งของวิชา 322222 เครือข่าย 1
(Network 1) Section 3ภาคการศึกษาที่ 2 ปีการศึกษาที่ 2559
ภาควิชาวิทยาการคอมพิวเตอร์
คณะวิทยาศาสตร์ มหาวิทยาลัยขอนแก่น

คำนำ

โครงงานการทดสอบความปลอดภัยบนเครือข่ายไร้สาย เป็นส่วนหนึ่งของรายวิชา 322222 เครือข่าย 1 จัดทำขึ้นเพื่อศึกษาการทดสอบความปลอดภัย ของระบบเครือข่ายไร้สาย โดยใช้เครื่องมือในการทดสอบ คือ Kali Linux

เพื่อให้ผู้อ่านได้นำข้อมูลจากโครงงานนี้ไปประยุกต์ใช้ได้ ไม่มากก็น้อย หากโครงงานนี้มีเนื้อหาใดที่ผิดพลาด หรือ ไม่ถูกต้อง ประการใดทางคณะผู้จัดทำใคร่ขออภัยไว้ ณ ที่นี้

คณะผู้จัดทำ

4 พฤษภาคม 2560

ชื่อหัวข้อโครงงาน : การทดสอบความปลอดภัยบนเครือข่ายไร้สาย

คณะผู้จัดทำโครงงาน :

1. นายทศพร ไชยชมภู รหัสนักศึกษา 583020160-0
2. นางสาวจุฑาทิพย์ ฐานวิสัย รหัสนักศึกษา 583020651-1
3. นางสาวศุภสุดา เรืองตระกูล รหัสนักศึกษา 583020683-8
4. นายเอกราช ศรีอาภรณ์ รหัสนักศึกษา 583021405-1
5. นายกันตพัฒน์ ทิพย์พิมลธนา รหัสนักศึกษา 583021365-7
6. นายธนพล ศรีโยธี รหัสนักศึกษา 583020661-8

เกี่ยวกับโครงงาน : รายงานนี้เป็นส่วนหนึ่ง 322222 เครือข่าย 1

อาจารย์ที่ปรึกษาโครงงาน : รศ.ดร.จักรชัย โสอินทร์

บทคัดย่อ

โครงงานการทดสอบความปลอดภัยบนเครือข่ายไร้สาย จัดทำขึ้นเพื่อ ศึกษาถึงความปลอดภัยของระบบเครือข่ายไร้สาย ที่มีการใช้งานอย่างแพร่หลายในปัจจุบัน ทำให้ การศึกษาเรื่องนี้มีความสำคัญอย่างยิ่ง และสามารถนำความรู้ที่ได้ค้นคว้า นี้ไปประยุกต์ใช้กับสายงาน และชีวิตประจำวันได้

โดยโครงงานการทดสอบความปลอดภัยบนเครือข่ายไร้สาย ได้ดำเนินการทำโครงงานโดยวิธีการทดสอบระบบความปลอดภัยของเครือข่าย คือ Kali Linux ซึ่งเป็นระบบปฏิบัติการที่มีแพลทฟอร์ม ทางด้านระบบทดสอบความปลอดภัย การทดสอบเจาะระบบ

ซึ่งในการทดสอบในครั้ง นี้ โดยวิธี Hashcat และการเข้ารหัส โดยวิธี Brute Force เพื่อให้ได้มาซึ่งรหัสผ่าน สำหรับเข้าใช้งานเครือข่ายไร้สาย ซึ่งสามารถสรุปผลได้ดังนี้ ในการทดสอบพบว่า ในการ Hashcat เพื่อให้ได้แพกเกจนั้น สามารถทำได้ ก็ต่อเมื่อ มีผู้เข้ามาใช้งานเครือยข่ายนั้นอยู่เท่านั้น และ จะต้องนำไฟล์ ที่ได้จากการ Hashcat นั้นมาเข้ารหัสโดยวิธีการ Brute Force เพื่อเข้ารหัสโดยการสุ่มเรียงตัวอักษร ตัวเลข หรือ สัญลักษณ์ แต่ ความยากง่ายของรหัสนั้นมีผลต่อการ ถอดรหัส แบบ Brute Force อีกด้วย ซึ่งในการที่จะได้รหัสผ่านมานั้น จะสามรถทำได้ในกลุ่มเป้าหมายที่ มีปัจจัยเอื้อ การเข้าถึง ของเครื่องมือที่ใช้ในการทดสอบ

สารบัญ

บทที่ 1
บทนำ

ที่มาและความสำคัญของโครงงาน

เนื่องจากปัจจุบันเครือข่ายไร้สายมีการใช้งานอย่างแพร่หลาย รวมถึงมีการใช้อุปกรณ์ ที่ใช้เครือข่ายในการติดต่อสื่อสารระหว่างกัน ผ่านเครือข่ายไร้สายดังนั้น การติดตั้งเครือข่ายไร้สายจึงมีความจำเป็นที่จะต้องมีความปลอดภัย ส่งผลให้เครือข่ายมีประสิทธิภาพและตอบสนองความต้องการของผู้ใช้งานได้เป็นอย่างดี ทำให้เกิดเสถียรภาพ ในการใช้งาน

การทดสอบความปลอดภัยบนระบบเครือข่ายไร้สายจึงเป็นทางเลือกในการ ที่ดีในการทดสอบความปลอดภัยรวมถึงทดสอบระบบ ให้มีความมั่นคง จึงทำให้มีความปลอดภัยในการใช้งาน ในการทดสอบครั้งนี้ ได้นำเอาเครื่องมือในการทดสอบ เป็นซอฟต์แวร์ที่ใช้ในงานด้านความปลอดภัย Kali Linux มาใช้ในการทดสอบในครั้งนี้

วัตถุประสงค์

- เพื่อศึกษาความแตกต่างของ ความปลอดภัยแต่ละแบบในเครือข่ายไร้สาย
- เพื่อศึกษาการใช้ในงานเครื่องมือในการตรวจสอบความปลอดภัยบนเครือข่าย

ขอบเขตของการศึกษา

- การทดสอบความปลอดภัยของเครือข่ายไร้สาย โดยใช้เครื่องมือ KALI LINUX

ประโยชน์ที่คาดว่าจะได้รับ

- เพื่อศึกษาถึงความแตกต่างของ ความปลอดภัยแต่ละแบบในเครือข่ายไร้สายมาปรับใช้ให้เกิดประโยชน์
- เพื่อนำความรู้เรื่อง การใช้งานเครื่องมือในการตรวจสอบความปลอดภัยบนเครือข่าย มาปรับใช้ในชีวิตประจำวัน

บทที่ 2
เอกสารและงานวิจัยที่เกี่ยวข้อง

ในการทดสอบความปลอดภัยของเครือข่ายไร้สาย ได้นำเอาทฤษฎี ต่างที่เกี่ยวข้องกับโครงงานนนี้ ซึ่งมีหัวข้อดังต่อไปนี้

- เทคโนโลยีเครือข่ายไร้สาย
- มาตรฐาน IEEE 802.11
- Kali Linux

2.1) เทคโนโลยีเครือข่ายไร้สาย

เทคโนโลยีเครือข่ายไร้สาย

ในช่วงหลายปีที่ผ่านมาได้มีการพัฒนาแบบก้าวกระโดดของระบบคอมพิวเตอร์ โดยเฉพาะการพัฒนาทางด้านเน็ตเวิร์ก ไม่ว่าจะเป็นความเร็วในการสื่อสาร รูปแบบการให้บริการใหม่ๆ ความง่ายในการเชื่อมต่อ (ระบบปฏิบัติการช่วยสนับสนุน) การพัฒนาแบบก้าวกระโดดนี้มีผลจากการใช้งานของผู้ใช้มากขึ้น รวมถึงผู้ให้บริการต่างๆ ได้จัดบริการใหม่ๆ ที่รองรับการทำงานบนอินเทอร์เน็ตมากขึ้น สิ่งเหล่านี้จึงเป็นแรงผลักดันให้การพัฒนาทางด้านเน็ตเวิร์กรวดเร็วมากขึ้น และใกล้ตัวผู้ใช้มากขึ้นด้วยเช่นกัน

หากพูดถึงการส่งข้อมูลผ่านอากาศของระบบเครือข่ายคอมพิวเตอร์ไม่ว่าการใช้งานภายในออฟฟิศ บ้าน รวมถึงสถานที่ต่างๆ ยังเรียกได้ว่าเป็นสิ่งใหม่มาก เพราะมาตรฐานแรกสำหรับเน็ตเวิร์กแบบไร้สายก็เพิ่งออกมาในช่วงปี 2002 นั่นคือ 802.11b ซึ่งมาตรฐานนี้มีความเร็วในการรับส่งข้อมูลสูงสุดที่ 11 เมกะบิตต่อวินาที (Mbps) ในทางทฤษฎี แต่การใช้งานจริงนั้น ความเร็วจะไม่ถึงความเร็วสูงสุดที่มาตรฐานกำหนดขึ้น ซึ่งมีผลกระทบมากมายทั้งจาก เครื่องใช้ไฟฟ้ารอบข้าง อุปกรณ์มือถือ เครื่องไมโครเวฟ และรูปแบบของอาคารด้วยเช่นกัน

ในปี 2004 เดือนมิถุนายนได้มีมาตรฐานเครือข่ายไร้สายใหม่ภายใต้ชื่อ 802.11g ซึ่งรองรับความเร็วสูงสุดที่ 54 Mbps แต่ยังคงทำงานที่ความถี่สัญญาณ 2.4 GHz เช่นเดียวกับ 802.11b และทั้งสองมาตรฐานนี้

ทำงานร่วมกันได้เช่นกัน (ต่างจากมาตรฐาน 802.11a ที่ความเร็ว 54 Mbps เช่นกันแต่ระยะทำงานสั้นกว่า และไม่สามารถใช้งานร่วมกับ 802.11b ได้) ร่วมถึงมีบางผลิตภัณฑ์ใช้เทคโนโลยีเฉพาะตัวเข้ามาเสริมทำให้ความเร็วเพิ่มขึ้นถึง 108 Mbps แต่ต้องทำงานร่วมกันเฉพาะอุปกรณ์ที่ผลิตจากบริษัทเดียวกันเท่านั้น

ระบบเครือข่ายไร้สายคืออะไร

ระบบเครือข่ายไร้สาย (Wireless LAN : WLAN) หมายถึง เทคโนโลยีที่ช่วยให้การติดต่อสื่อสารระหว่างเครื่องคอมพิวเตอร์ 2 เครื่อง หรือกลุ่มของเครื่องคอมพิวเตอร์สามารถสื่อสารกันได้ ร่วมถึงการติดต่อสื่อสารระหว่างเครื่องคอมพิวเตอร์กับอุปกรณ์เครือข่ายคอมพิวเตอร์ด้วยเช่นกัน โดยปราศจากการใช้สายสัญญาณในการเชื่อมต่อ แต่จะใช้คลื่นวิทยุเป็นช่องทางการสื่อสารแทน การรับส่งข้อมูลระหว่างกันจะผ่านอากาศ ทำให้ไม่ต้องเดินสายสัญญาณ และติดตั้งใช้งานได้สะดวกขึ้น

Technology Wi-Fi

ระบบเครือข่ายไร้สายใช้แม่เหล็กไฟฟ้าผ่านอากาศ เพื่อรับส่งข้อมูลข่าวสารระหว่างเครื่องคอมพิวเตอร์และระหว่างเครื่องคอมพิวเตอร์กับอุปกรณ์เครือข่าย โดยคลื่นแม่เหล็กไฟฟ้านี้อาจเป็นคลื่นวิทย (Radio) หรืออินฟาเรด (Infrared) ก็ได้

การสื่อสารผ่านเครือข่ายไร้สายมีมาตราฐาน IEEE802.11 เป็นมาตราฐานกำหนดรูปแบบการสื่อสาร ซึ่งมาตราฐานแต่ละตัวจะบอกถึงความเร็วและคลื่นความถี่สัญญาณที่แตกต่างกันในการสื่อสารข้อมูล เช่น 802.11b และ 802.11g ที่ความเร็ว 11 Mbps และ 54 Mbps ตามลำดับ สามารถศึกษารายละเอียดเพิ่มเติมศึกษาได้จาก มาตราฐาน IEEE802.11 และขอบเขตของสัญญาณคลอบคุลพื้นที่ประมาณ 100 เมตร ในพื้นที่โปรง และประมาณ 30 เมตร ในอาคาร ซึ่งระยะทางของสัญญาณมีผลกระทบจากสิ่งรอบข้างหลายๆ อย่าง เช่น โทรศัพท์มือถือ ความหนาของกำแพง เครื่องใช้ไฟฟ้า อุปกรณ์อิเล็กทรอนิคส์ต่างๆ รวมถึงร่างกายมนุษย์ด้วยเช่นกัน สิ่งเหล่านี้มีผลกระทบต่อการใช้งานเครือข่ายไร้สายทั้งสิ้น

การเชื่อมต่อเครือข่ายไร้สายมี 2 รูปแบบ คือแบบ Ad-Hoc และ Infrastructure รายละเอียดเพิ่มเติมศึกษาได้จาก รูปแบบเครือข่ายไร้สาย การใช้งานเครือข่ายไร้สายของผู้ใช้บริการทั่วไปจะเป็นแบบ Infrastructure คือมีอุปกรณ์กระจายสัญญาณ (Access Point) ของผู้ให้บริการเป็นผู้ติดตั้งและกระจายสัญญาณ ให้ผู้ใช้ทำการเชื่อมต่อ โดยผู้ใช้บริการจะต้องมีอุปกรณ์รับส่งสัญญาณขอเรียกว่า "การ์ดแลนไร้สาย" เป็นอุปกรณ์รับส่งสัญญาณ ทำหน้าที่รับส่งสัญญาณจากเครื่องคอมพิวเตอร์ผู้ใช้ไป Access Point ของผู้ให้บริการ

สรุปการเชื่อมต่อเครือข่ายไร้สายเป็นการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์เข้าสู่ระบบเครือข่าย เหมือนกับระบบแลน (LAN) มีสายปกติ แตกต่างที่อุปกรณ์ทางกายภาพในการเชื่อมต่อเครือข่ายไม่ต้องใช้สายสัญญาณแต่อย่างใด โดยการใช้งานเครือข่ายไร้สายสามารถใช้บริการต่างๆ บนเครือข่ายอินเทอร์เน็ตได้เหมือนเครือข่ายมีสายได้ปกติ เว้นแต่ว่าผู้ดูแลระบบเครือข่ายนั้นๆ จะปิดบริการบางบริการเพื่อความปลอดภัยของเครือข่ายได้เช่นกัน ซึ่งการเชื่อมต่อเครือข่ายไร้สายช่วยให้การเชื่อมต่อง่ายขึ้น ประหยัดค่าสายสัญญาณ และใช้งานได้ทุกที่ที่สัญญาณเครือข่ายไร้สายไปถึง

ประโยชน์เครือข่ายไร้สาย

การเจริญเติบโตของเครือข่ายไร้สายเกิดขึ้นอย่างรวดเร็วนับตั้งแต่มีมาตราฐาน 802.11 เกิดขึ้น ระบบเครือข่ายไร้สายได้ถูกพัฒนาอย่างต่อเนื่อง ปัจจุบันนี้เครือข่ายไร้สายสามารถใช้งานได้สะดวก และมีความปลอดภัยมากขึ้น และที่สำคัญความเร็วในการสื่อสารสูงถึง 54 Mbps

- มหาวิทยาลัยสามารถใช้เครือข่ายไร้สายโดยนักศึกษาสามารถเข้าถึงบทเรียน Online ต่างๆ ได้ สามารถสืบค้นข้อมูลบนอินเทอร์เน็ตจากจุดใดจุดหนึ่งของสถาบันได้ และนักศึกษาไม่จำเป็นต้องรอเข้าใช้ห้องบริการคอมพิวเตอร์ของสถาบัน สามารถใช้จากจุดใดก็ได้ที่สัญญาณเครือข่ายไร้สายไปถึง ช่วยให้นักศึกษาสามารถใช้งานได้สะดวกและรวดเร็วมากขึ้น

- ผู้ให้บริการเครือข่ายไร้สายลดค่าใช้จ่ายในการเดินสายสัญญาณให้เข้าถึงจุดบริการต่างๆ มากขึ้น และสามารถให้บริการในจุดบริการที่สายสัญญาณไม่สามารถเข้าถึงได้เช่นกัน

- ผู้บริหารจัดการระบบเครือข่าย สามารถเผ้าตรวจสอบระบบ และปรับเปลี่ยนแก้ไขปัญหาที่อาจเกิดขึ้นกับระบบเครือข่ายจากจุดก็ได้ ทำให้สะดวกและรวดเร็วต่อการจัดการมากขึ้น

- ด้านธุรกิจผู้ดูแลสต๊อกสินค้า สามารถตรวจสอบข้อมูลสินค้าต่างๆ ในสต๊อกกับฐานข้อมูลกลางจากที่ใดในโกดังได้ทุกที่ตลอดเวลา

- ผู้ใช้งานสามารถทำงานได้ทุกสถานที่ตามที่ต้องการ ทำให้ผลิดผลของงานเพิ่มมากขึ้นด้วยเช่นกัน ปัจจุบันความนิยมใช้งานเครือข่ายไร้สายเพิ่มขึ้น เกิดจากการรองรับของอุปกรณ์ WLAN เพิ่มจำนวนขึ้น เช่น โน้ตบุ๊ค (Notebook) และพีดีเอ (PDA) อย่างเช่นโน้ตบุ๊ครุ่นใหม่ที่ผลิดขึ้นจะสามารถใช้งานเครือข่ายไร้สายได้โดยไม่ต้องมีการ์แลนไร้สายช่วยแต่อย่างใด ที่รู้จักในชื่อ centrino ขณะที่พีดีเอต้องมีอุปกรณ์เสริมจึงจะสามารถใช้งานเครือข่ายไร้สายได้ และสามารถสังเกตุได้จากห้างสรรพสินค้า ร้านกาแฟ โรงแรม สนามบิน ที่ให้บริการ WLAN เพิ่มขึ้นในหลายๆ ที่ แสดงให้เห็นถึงต้องการใช้เครือข่ายไร้สายเพิ่มมากขึ้นเช่นกัน (สามารถ

ตรวจสอบจุดบริการ Wireless ได้จาก จุดบริการ Wireless ในกรุงเทพฯ และจุดบริการ Wireless ในต่างจังหวัด)

อ้างอิง :

Nakornb. *เทคโนโลยีเครือข่ายไร้สาย* .เว็บไซต์ : http://chilchil.swu.ac.th.ปีที่ : 2551
แหล่งที่มา : http://chilchil.swu.ac.th/wiki/index.php/%E0%B9%80%E0%B8%84%E0%B8%A3%E0%B8%B7%E0%B8%AD%E0%B8%82%E0%B9% , เข้าถึงเมื่อ 4 พฤษภาคม 2560.

2.2) มาตรฐาน IEEE 802.11

Institute of Electrical and Electronics Engineers (IEEE) เป็นองค์กรกำนหดมาตรฐานการสื่อสารข้อมูลบนระบบเครือข่ายคอมพิวเตอร์ ซึ่งได้กำหนดมาตรฐานสำหรับเครือข่ายไวเลสแลนขึ้น คือ มาตรฐาน IEEE802.11 และกำหนดมาตรฐานย่อยขึ้น คือ a, b, g และ n ตามลำดับ โดยแต่ละมาตรฐานมีความเร็วและคลื่นความถี่สัญญาณที่แตกต่างกัน มีรายละเอียดดังนี้

2.2.1) มาตรฐาน IEEE 802.11a

เครือข่ายไวเลสแลนที่ทำงานย่านความถี่ 5 GHz มีความเร็วในการรับส่งข้อมูล 54 Mbps สามารถทำการแพร่ภาพวิดีโอและข้อมูลที่ต้องการความละเอียดสูงได้ โดยอัตราความเร็วในการรับส่งข้อมูลสามารถปรับระดับให้ช้าลงได้ เพื่อเพิ่มระยะทางการเชื่อมต่อให้มากขึ้น เช่น 54, 48, 36, 24 และ 11 Mbps เป็นต้น ขณะที่คลื่นความถี่ 5 GHz ไม่ได้ใช้งานอย่างแพร่หลาย เพราะบางประเทศไม่อนุญาติให้ใช้คลื่นความถี่นี้ ดังนั้นปัญหาการรบกวนคลื่นความถี่จึงมีน้อย ต่างจากคลื่นความถี่ 2.4 GHz ที่มีการใช้งานอย่างแพร่หลายทำให้สัญญาณของคลื่นความถี่ 2.4 GHz ถูกรบกวนจากอุปกรณ์ประเภทอื่นที่ใช้คลื่นความถี่เดียวกันได้

ระยะทางการเชื่อมต่อประมาณ 300 ฟิตจากจุดกระจายสัญญาณ Access Point หากเทียบกับมาตรฐาน 802.11b แล้ว ระยะทางจะได้น้อยกว่า 802.11b ที่คลื่นความถี่ต่ำกว่า และทั้ง 2 มาตรฐานนี้ไม่สามารถทำงานร่วมกันได้ ขณะที่ประเทศไทยไม่อนุญาติให้ใช้คลื่นความถี่ 5 GHz จึงไม่เห็นอุปกรณ์ WLAN มาตรฐาน 802.11a จำหน่ายในประเทศไทย แต่ความเร็ว 54 Mbps สามารถใช้งานได้ที่มาตรฐาน 802.11b ที่จะกล่าวถึงต่อไป

2.2.2) มาตรฐาน IEEE 802.11b

802.11b เป็นมาตรฐานที่ได้รับความนิยมอย่างแพร่หลายรวมทั้งประเทศไทยด้วยเช่นกัน ทำงานที่คลื่นความถี่ 2.4 GHz (คลื่นความถี่นี้สามารถใช้งานแบบสาธารณะในประเทศไทยได้) มีความสามารถในการรับส่งข้อมูลที่ความเร็ว 11 Mbps ผลิตภัณฑ์อุปกรณ์เครือข่ายไวเลสแลนมาตรฐานนี้ได้รับความนิยมจำนวนมากมาก โดยทุกผลิตภัณฑ์ต้องสามารถทำงานร่วมกันได้ อุปกรณ์ทุกยี่ห้อต้องผ่านการตรวจสอบจากสถาบัน Wi-Fi Alliance เพื่อตรวจสอบมาตรฐานของอุปกรณ์และความเข้ากันได้ของแต่ละผู้ผลิต

อุปกรณ์ไวเลสแลนที่มาตรฐาน 802.11b ไปใช้ในองค์กรธุรกิจ สถาบันการศึกษา สถานที่สาธารณะ และกำลังแพร่เข้าสู่สถานที่พักอาศัยมากขึ้น และมาตรฐานนี้มีระบบเข้ารหัสข้อมูลแบบ WEP ที่ 128 บิต

2.2.3) มาตรฐาน IEEE 802.11g

มาตรฐาน 802.11g ใช้ความถี่ 2.4 GHz สามารถรับส่งข้อมูลที่ความเร็ว 36 - 54 Mbps ซึ่งเป็นความเร็วที่สูงกว่ามาตรฐาน 802.11b โดยมาตรฐาน 802.11g สามารถปรับระดับความเร็วในการสื่อสารลงเหลือ 2 Mbps ได้ (ตามสภาพแวดล้อมของเครือข่ายที่ใช้งาน) มาตรฐานนี้เป็นที่นิยมของผู้ใช้เป็นจำนวนมากและเข้ามาแทนที่ 802.11b ที่ความเร็วต่ำกว่า

2.2.4) มาตรฐาน IEEE 802.11n

เป็นมาตรฐานที่สามารถทำงานบนคลื่นความถี่ 2.4 และ 5 GHz ได้ รองรับความเร็วตั้งแต่ 300-450 Mbps โดยมีเสาสัญญาณตั้งแต่ 2 - 4 เสา บนตัวอุปกรณ์กระจายสัญญาณไวเลสแลน และหากผู้ใช้ต้องการใช้งานที่ความเร็วสูงสุด เครื่องคอมพิวเตอร์พกพาหรืออุปกรณ์เคลื่อนที่ต้องรองรับมาตรฐาน 802.11n ด้วยเช่นกัน มาตรฐาน 802.11n สามารถทำงานร่วมกับ 802.11b, g ได้ โดยไม่ทำให้ประสิทธิภาพทั้งระบบลดลงเหมือนมาตรฐาน 802.11g เมื่อมีอุปกรณ์ 802.11b เข้ามาใช้งานร่วมกัน สุดท้าย

นอกจากที่กล่าวมาข้างต้นแล้ว ยังมีบางผลิตภัณฑ์ใช้เทคโนโลยีเฉพาะตัวเข้ามาเสริมช่วยทำให้ความเร็วเพิ่มขึ้นจาก 54 Mbps เป็น 108 Mbps แต่ต้องเป็นอุปกรณ์ที่ผลิตจากบริษัทเดียวกันเท่านั้น ซึ่งความสามารถนี้เกิดจากชิพ (Chip) กระจายสัญญาณไวเลสของตัวอุปกรณ์เพิ่มประสิทธิภาพการรับส่งสัญญาณเป็น 2 เท่าได้ แต่ปัญหาของการกระจายสัญญาณนี้จะมีผลทำให้อุปกรณ์ไร้สายในมาตรฐาน 802.11b มีประสิทธิภาพลดลงด้วยเช่นกัน

[illegible]	คลื่นความถี่	[illegible]
802.11a	5.1-5.2 GHz	54 Mbps
802.11b	2.4-2.8 GHz	11 Mbps
802.11g	2.4-2.8 GHz	36-54 Mbps
802.11n	2.4-5 GHz	300-450 Mbps

ตารางมาตรฐาน IEEE802.11 ของเครือข่ายไร้สาย

อ้างอิง

Srinakharinwirot University.. *มาตรฐาน IEEE 802.11* .เว็บไซต์ : http://wise.swu.ac.th/.ปีที่ : 2001 แหล่งที่มา : http://wise.swu.ac.th/Default.aspx?tabid=3440 , เข้าถึงเมื่อ 4 พฤษภาคม 2560.

2.3) Kali Linux

Offensive Security ผู้ผลิต BackTrack เปิดตัวระบบปฏิบัติการ Kali Linux สำหรับการทดสอบเจาะระบบ สำหรับผู้ที่มีอาชีพในการทดสอบเจาะระบบเพื่อตรวจสอบความปลอดภัย รวมไปถึงผู้ที่สนใจย่อมคุ้นเคยกับชื่อ BackTrack ดีอยู่แล้ว มันเป็นระบบปฏิบัติการลินุกซ์ซึ่งได้รับความนิยมอย่างแพร่หลายในการใช้งานด้านความปลอดภัย สำหรับตอนนี้ทาง Offensive Security ทีมผู้พัฒนา BackTrack ได้เปิดตัวระบบปฏิบัติการขึ้นใหม่ภายใต้ชื่อ Kali Linux โดยมุ่งไปยังกลุ่มเป้าหมายระดับในธุรกิจ

Kali Linux ในเวอร์ชันแรกนี้มีความแตกต่างจาก BackTrack ตรงที่ Kali Linux ได้เชื่อมต่อโดยตรงกับ repositories ของทาง Debian ซึ่งทำให้การอัพเดตนั้นง่ายขึ้นและประหยัดเวลาลง รองรับการปรับแต่งตัวระบบปฏิบัติการเพื่อสร้างเวอร์ชันที่เหมาะสำหรับตัวผู้ใช้เอง อีกทั้งยังรองรับการทำงานของ ARM ทำให้สามารถติดตั้งได้ทั้งบน Chromebook, Raspberry Pi หรือแท็บเลต รวมถึงสามารถพัฒนาโปรเจคทางด้านฮาร์ดแวร์ได้จากเครื่องมือที่ถูกเตรียมมาแล้วได้อีกด้วย ซึ่งแน่นอนว่ายังรองรับหลากหลาย desktop environments แล้วแต่ผู้ใช้งาน

อ้างอิง

Srinakharinwirot University.. *มาตรฐาน IEEE 802.11* .เว็บไซต์ : http://wise.swu.ac.th/.ปีที่ : 2001 แหล่งที่มา : http://wise.swu.ac.th/Default.aspx?tabid=3440 , เข้าถึงเมื่อ 4 พฤษภาคม 2560.

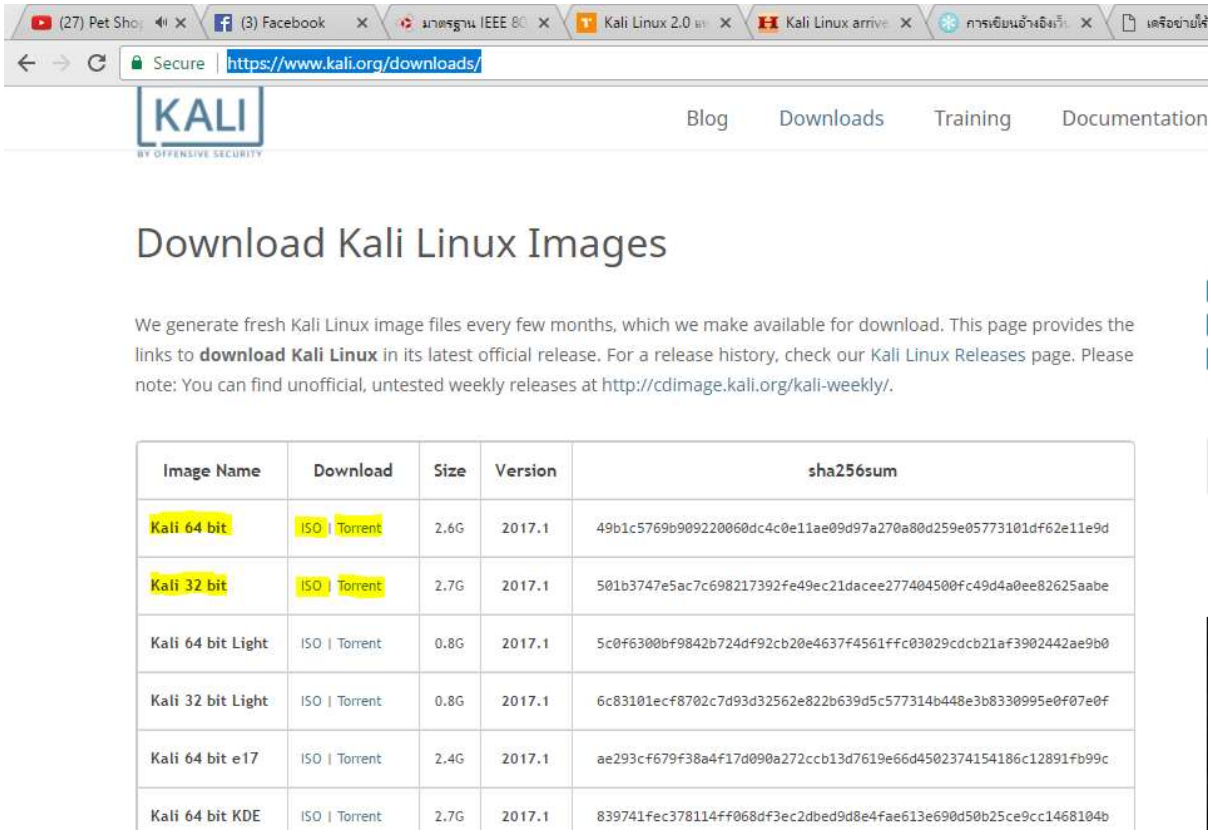
บทที่ 3
วิธีการดำเนินงาน

ในการทดสอบความปลอดภัยของระบบเครือข่ายไร้สาย ต้องมีเครื่องมือที่ใช้ในการทดสอบดังต่อไปนี้ คือ Kali Linux ในการทดสอบ สามารถแบ่งขั้นตอนในการดำเนินงานดังต่อไปนี้

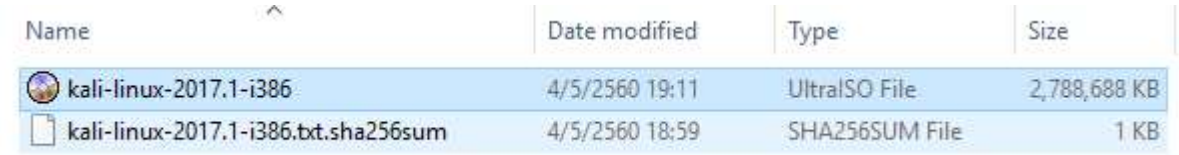
3.1) การเตรียมเครื่องมือในการทดสอบ

3.1.1) การเตรียม Kali Linux

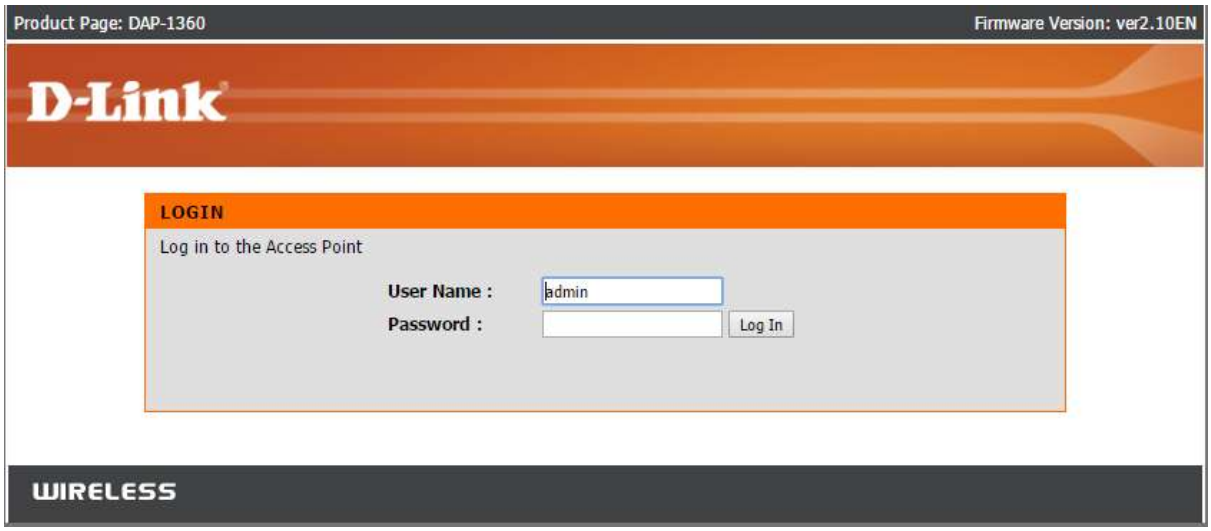
โดยการ ดาวน์โหลด จาก https://www.kali.org/downloads/



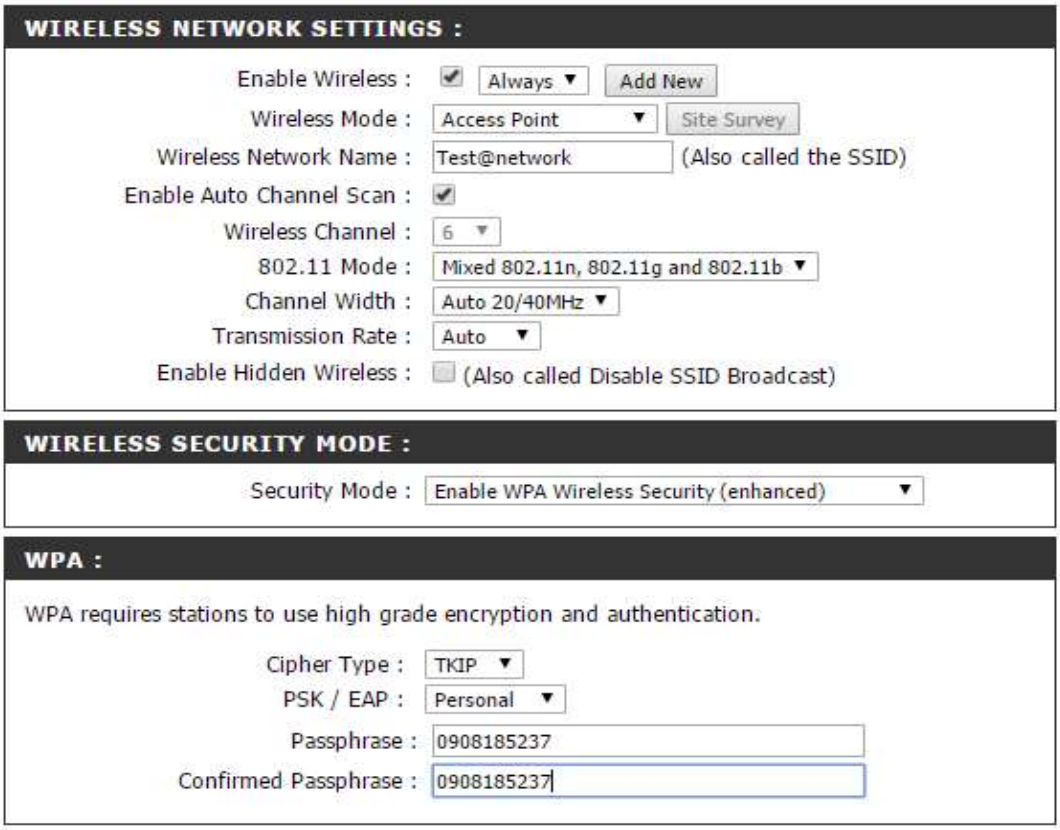
3.1.2) เตรียม ทำบูตผ่าน USB



3.1.2) เตรียม อุปกรณ์ Access Point ในการทดสอบ ในที่นี้ใช้ D-Link DAP 1360



ตั้งค่าอุปกรณ์ และ ตั้งค่าความปลอดภัย แต่ละชนิด



3.2) ขั้นตอนการทดสอบระบบเครือข่ายไร้สาย แบบ WPA

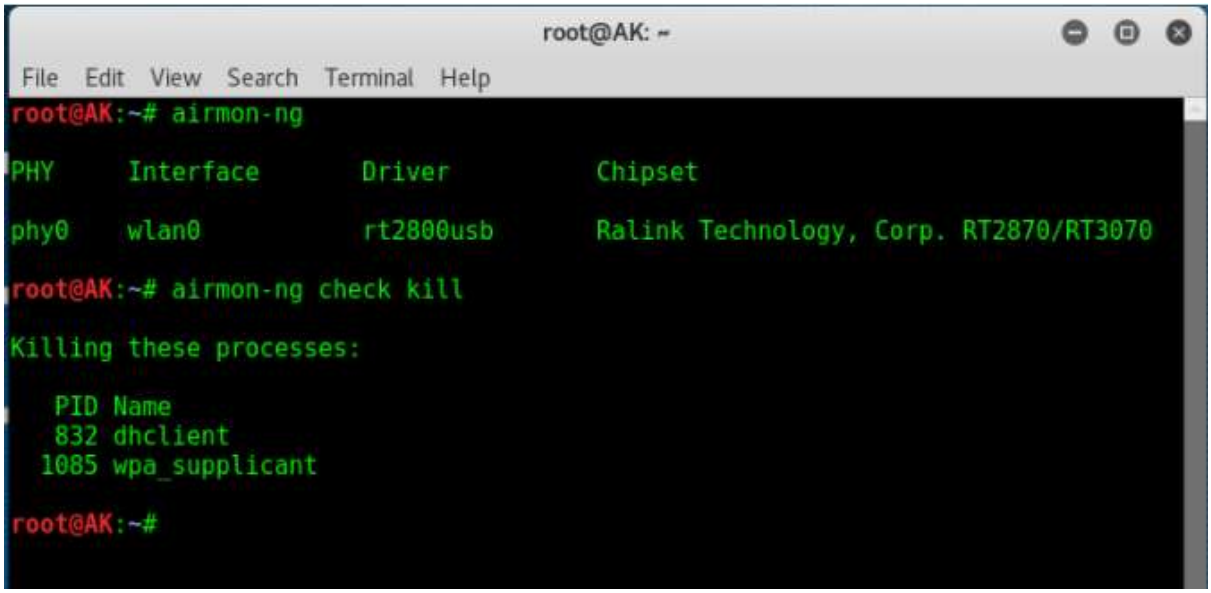
ในกรณีที่ มีอุปกรณ์ ไร้สายชนิดภายนอก หรือ แบบ USB wireless สามารถใช้ เครื่องในการจำลองเครื่องคอมพิวเตอร์ เสมือน เช่น Visual BOX หรือ VM WARE ในการจำลอง เครื่องสำหรับ ระบบ Kali Linux เพื่อใช้ในการทดสอบ ด้วย วิธีการแชร์ ฮาร์ดแวร์จากเครื่องหลัก ให้กับเครื่องเสมือน เพื่อให้สามารใช้ อุปกรณ์ที่ใช้ในการเชื่อมต่อเครือข่ายไร้สายร่วมกันได้

3.2.1) ติตตั้ง หรือ เริ่มการทำงานของ Kali Linux ทดสอบ โดยใช้ประเภทความความปลอดภัย แบบ WPA

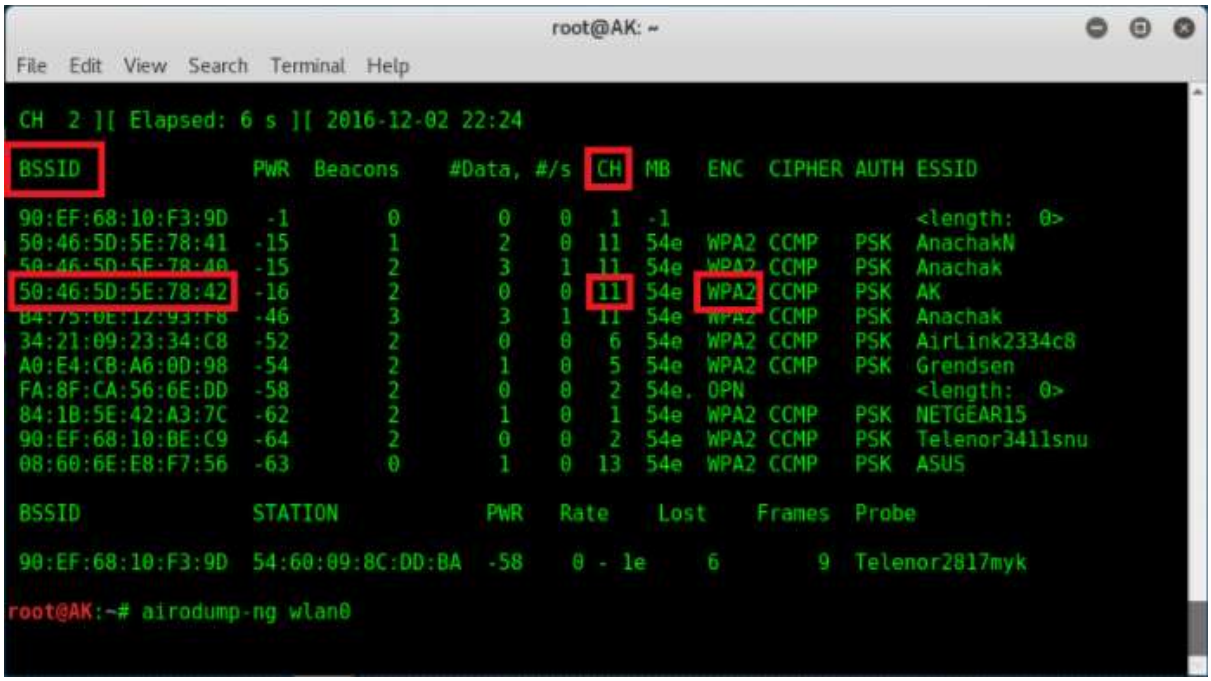
3.2.1) การทดสอบความปลอดภัยของเครือข่ายไร้สาย โดยวิธีการ Hashcat

เปิด Terminal ขึ้นมาแล้วให้ทดสอบก่อนว่า Wifi สามารถใช้การได้หรือไม่ด้วยคำสั่ง airmon-ng

และ ใช้คำสั่ง airmon-ng check kill เพื่อหยุดการทำงานของโปรเซส



ให้ใช้คำสั่ง airodump-ng wlan0 เพื่อค้นหาเครือข่ายที่ต้องการทดสอบความปลอดภัย



ให้ Copy BSSID (50:46:5D:5E:78:42) และจำ Channel (CH) ด้วยว่าเครือข่ายที่จะทำการ Hashcat ใช้ ช่องใด อยู่ (ปกติจะมี 1-14)

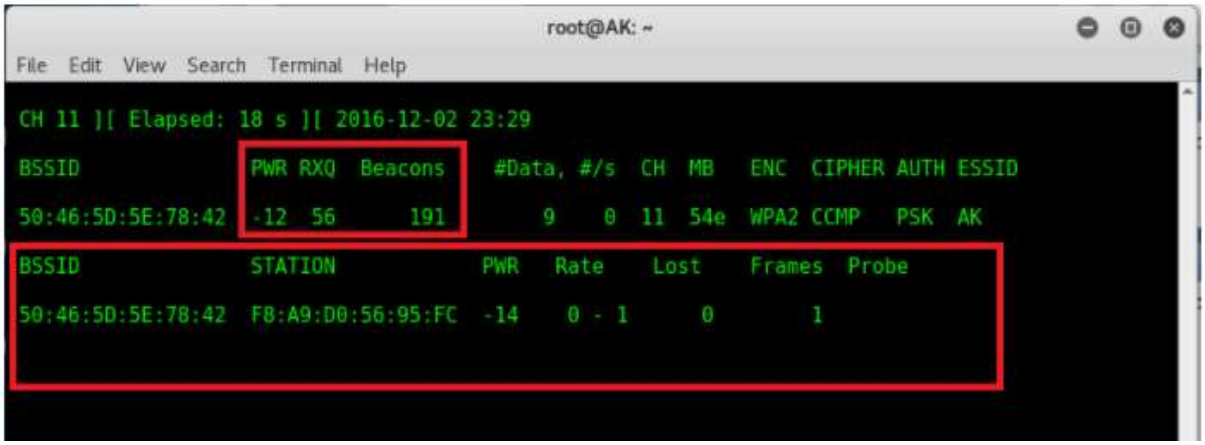
ขั้นตอนต่อไปให้เปิด Terminal ขึ้นมาใหม่หรือใช้อันเดิมก็ได้และใส่คำสั่งตามนี้

airodump-ng -w ak -c 11 --bssid 50:46:5D:5E:78:42 wlan0

-w ak หมายถึงให้เขียน cap file ชื่อ ak (จะอยู่ใน Home)

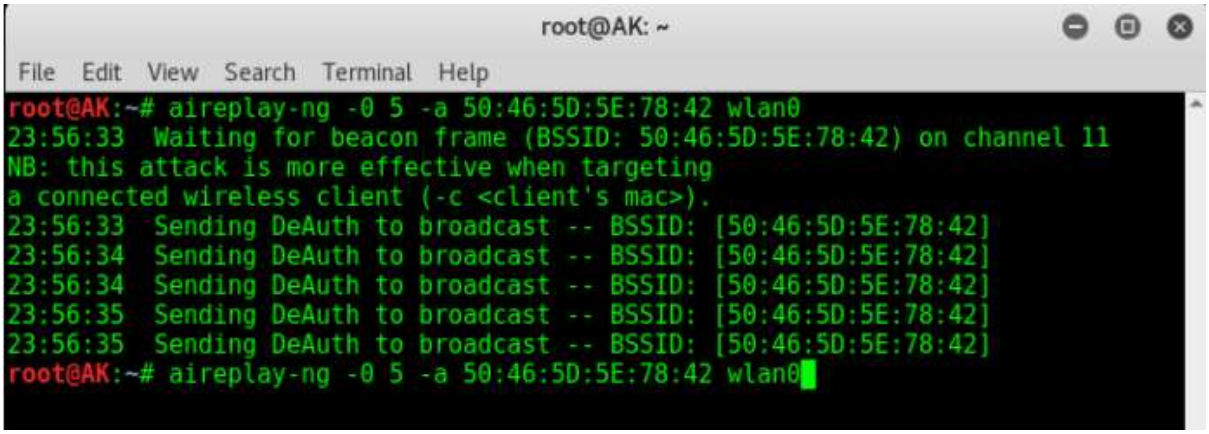
-c 11 หมายถึงช้องของ CH

–bssid หมายถึง MAC Address ของ AP ที่เราอยากทำการ Injection

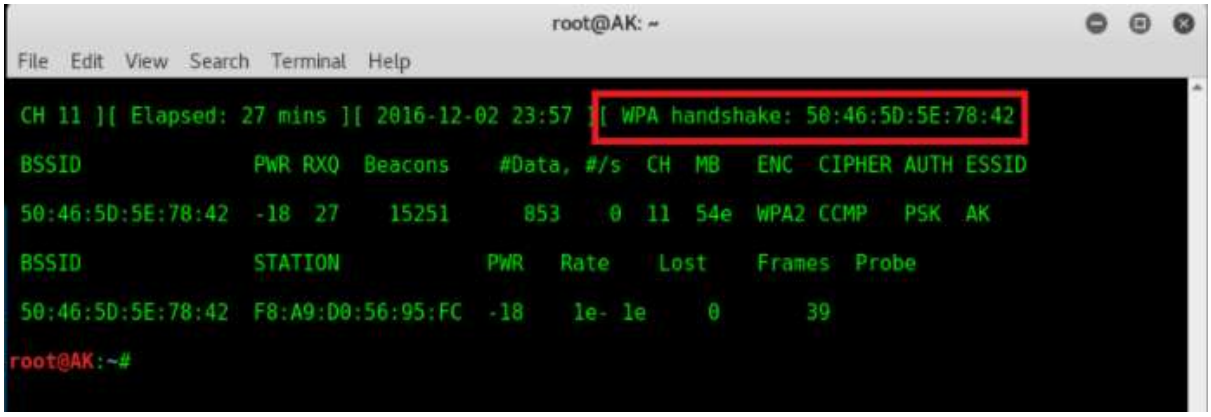


ขั้นตอนต่อไป เป็นการ Deauthenticate เพื่อให้อุปกรณ์ที่เชื่อมต่ออยู่ทำการเชื่อมต่อใหม่ และดักจับ Packets เพื่อทำการ Handshake. ให้ทำการเปิด Terminal ใหม่ขึ้น Terminal ที่รันอยู่ห้ามปิดเด็ดขาด.

ใน Terminal ใหม่ให้ใส่คำสั่งตามนี้ aireplay-ng -0 5 -a 50:46:5D:5E:78:42 wlan0



หากทำการยิงแพกเกจ ไปแล้ว ถ้ามี ผู้ที่ใช้งานเครือข่ายนี้อยู่ จึงจะสามารถ ดักจับแพกเกจ ได้



หากการดักจับแพกเกจ สำเร็จ จะ ปรากฏข้อความ WPA handshake: [BSSID]

ในขั้นตอนต่อไปคือการ ถอดรหัสจากไฟล์ ที่ได้จากการ Hashcat จากขั้นตอนข้างต้นการทำ Brute Force คือการที่เราไม่ต้องมี Wordlist แต่จะรันรหัสตามตัวเลขหรือตัวอักษรที่เราต้องการได้ โดยการขอใช้ Script CRUNCH. คำสั่งที่ใช้คือ

```
crunch 10 10 0123456789 | aircrack-ng ak.cap -w - -b 50:46:5D:5E:78:42
```

หรือถ้าเราอยากจะรันและให้ตัวหน้าหรือตัวใหนก็ได้ ให้เป็นตัวเริ่มต้นหรือตัวที่ต้องการก็ได้ตามนี้

```
crunch 10 10 0123456789 -t 08@@@@@@@@ | aircrack-ng ak.cap -w - -b 50:46:5D:5E:78:42
```

curnch หมายถึงการขอใช้งาน Script crunch 10 ตัวหน้าหมายถึงจำนวนหลักต่ำสุดกี่ตัว และ 10 ตัวหลังคือสูงสุดมีจะนวนกี่หลัก. ตัวอย่างเช็น 8 10 ก็หมายความว่า น้อยสุด 8 ตัว มากสุด 10 ตัว. 0123456789 คือตัวที่เราอยากจะให้รันถ้าจะให้รัน abc ก็ใส่เข้าไปก็จะเป็น crunch 10 10 abc123

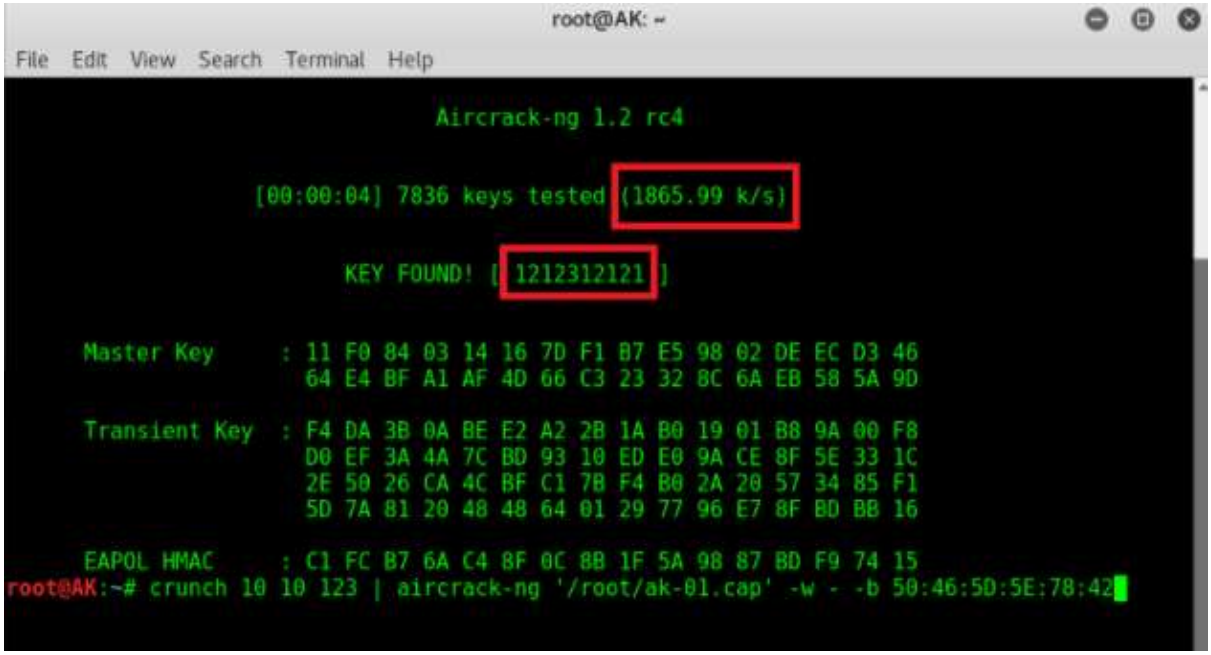
| หมายถึงการส่งค่าไป aircrack-ng คือการเรียกใช้

-w คือเปิดใช้ word ที่รับมา

– เป็นการเชื่อม

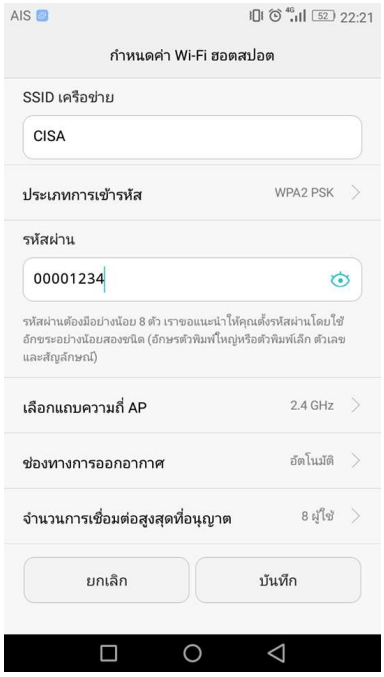
-b คือใช้ Mac Address ของเหยื่อที่เราทำ Handshake

ซึ่งจากขั้นตอนนี้จำทำให้สามารถถอดรหัส และ ได้ข้อความที่เป็นรหัสผ่านในการเข้า ยืนยันตัวตน ในเข้าใช้งานเครือข่าย Wireless Lan ได้



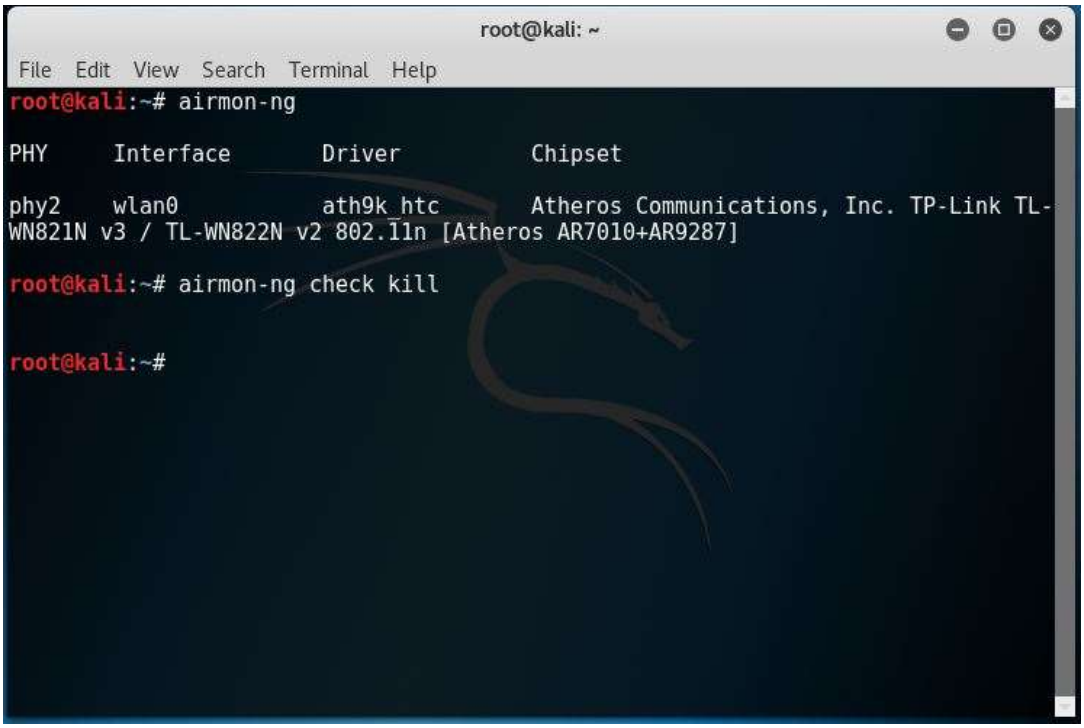
3.3) ขั้นตอนการทดสอบระบบเครือข่ายไร้สาย แบบ WPA2 / PSK

ในการทดสอบ เครือข่ายแบบไร้สายที่ใช้ระบบความปลอดภัยแบบ WPA2/PSK ในที่นี้ขอยกเอาเครือข่าย โดยใช้อุปกรณ์ สมาทโฟน ในการ ทำหน้าที่เป็น Access Point ในการกระจายสัญญาณ

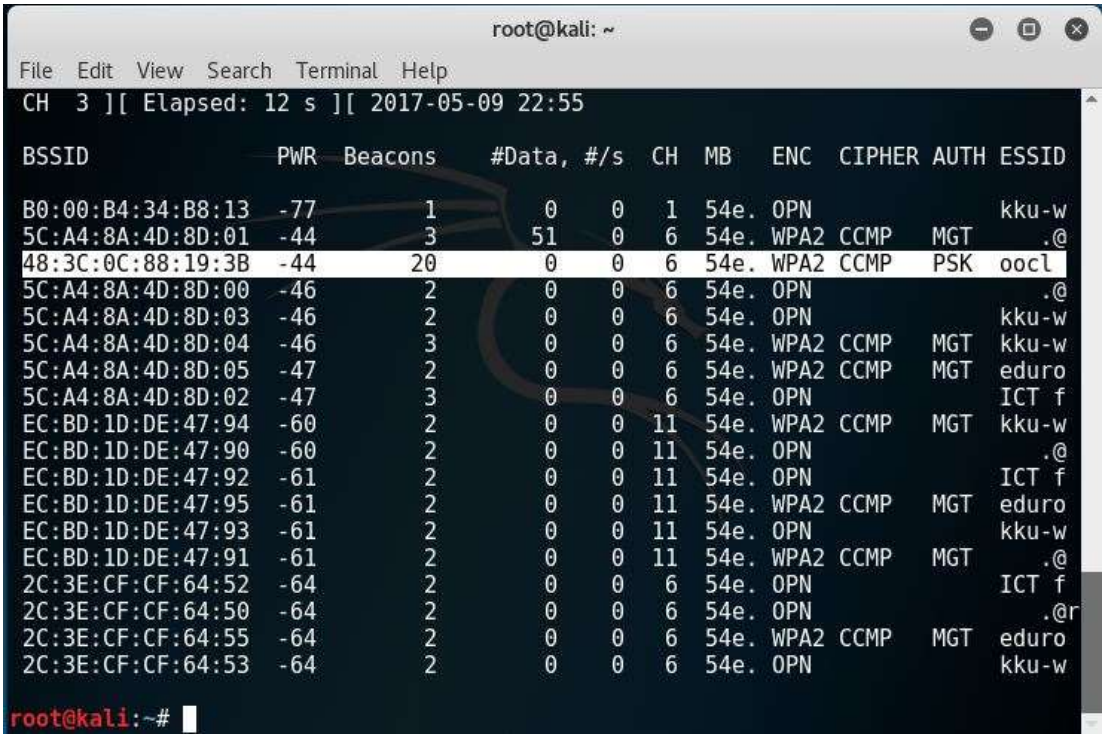


โครงงานการทดสอบความปลอดภัยบนเครือข่ายไร้สาย

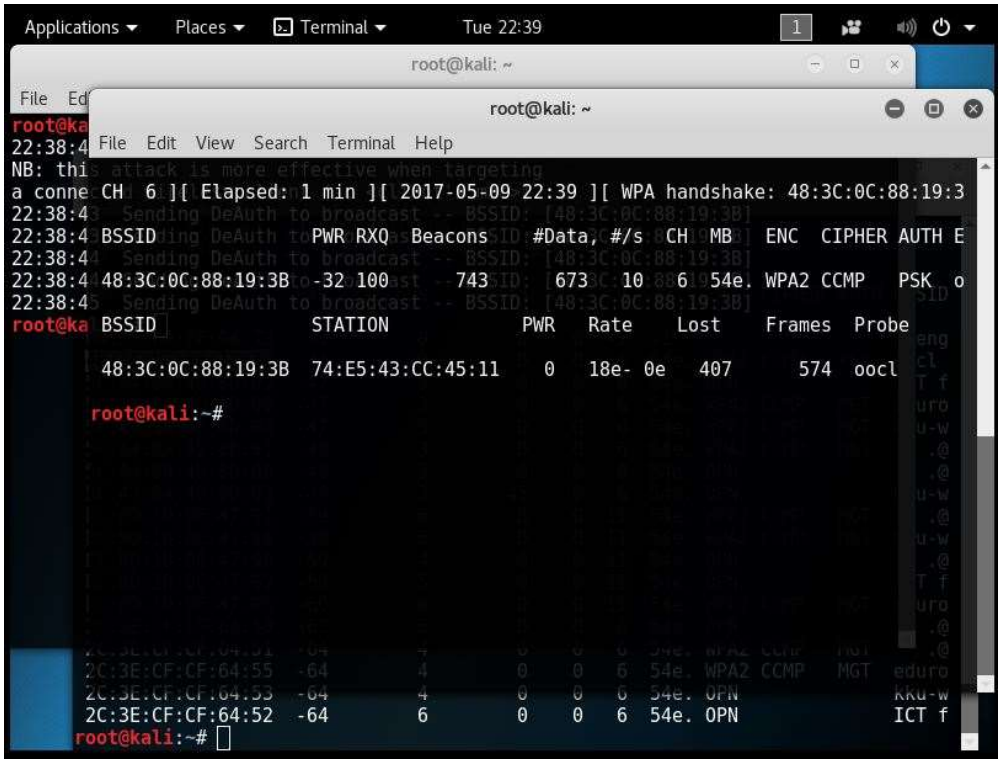
3.3.1) การทดสอบความปลอดภัยของเครือข่ายไร้สายแบบ WPA 2 / PSK โดยวิธีการ Hashcat



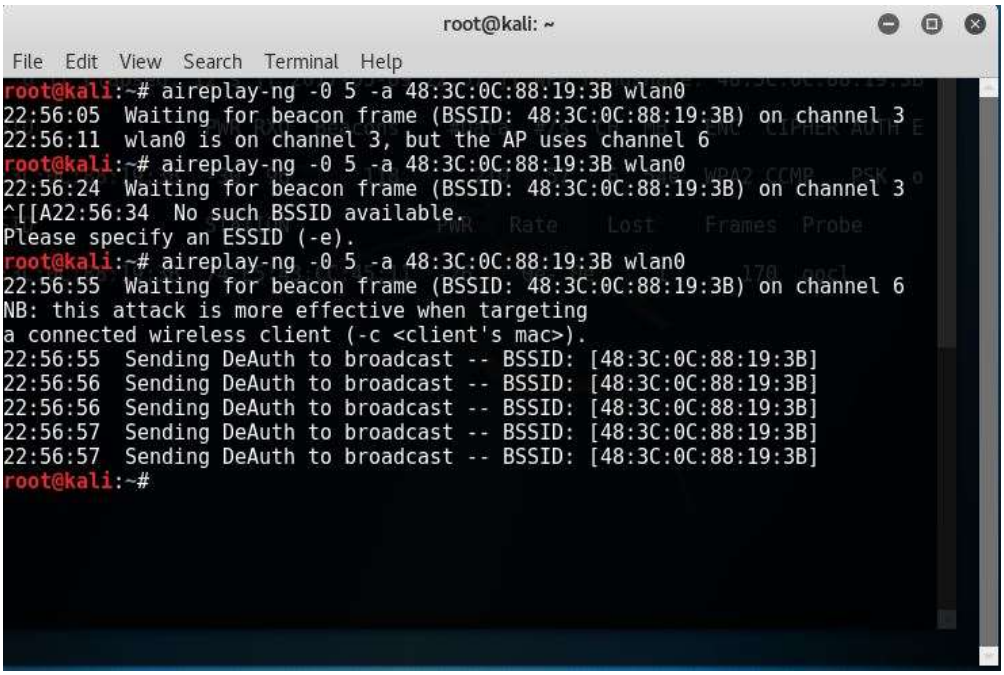
ขั้นแรกใช้คำสั่ง airmon-ng เพื่อเช็คว่ามีอุปกรณ์ในการเชื่อมต่อเครือข่ายไร้สายอยู่หรือไม่ จากนั้นใช้คำสั่ง ในการตรวจสอบ โปรเซสที่ทำงาน แล้วสั่งหยุดการทำงาน โปรเซส กับอุปกรณ์สำหรับเชื่อมต่อเครือข่ายไร้สาย ที่เชื่อมต่ออยู่

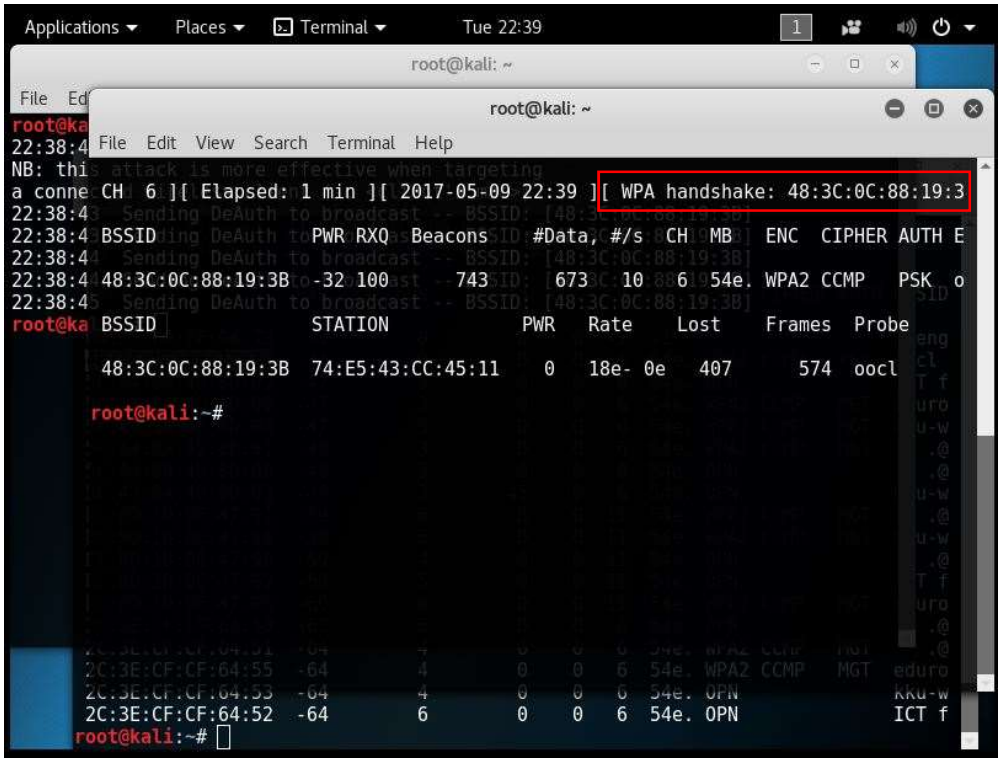


ขั้นตอนนี้ให้ทำการใช้คำสั่ง airodump-ng wlan0 เพื่อค้นหาเครือข่ายที่ต้องการจะทำการดักจับแพกเก็จ จากนั้นให้ทำการ Coppy BSSID ของเครือข่ายที่ต้องการดักจับแพ็กเก็จ

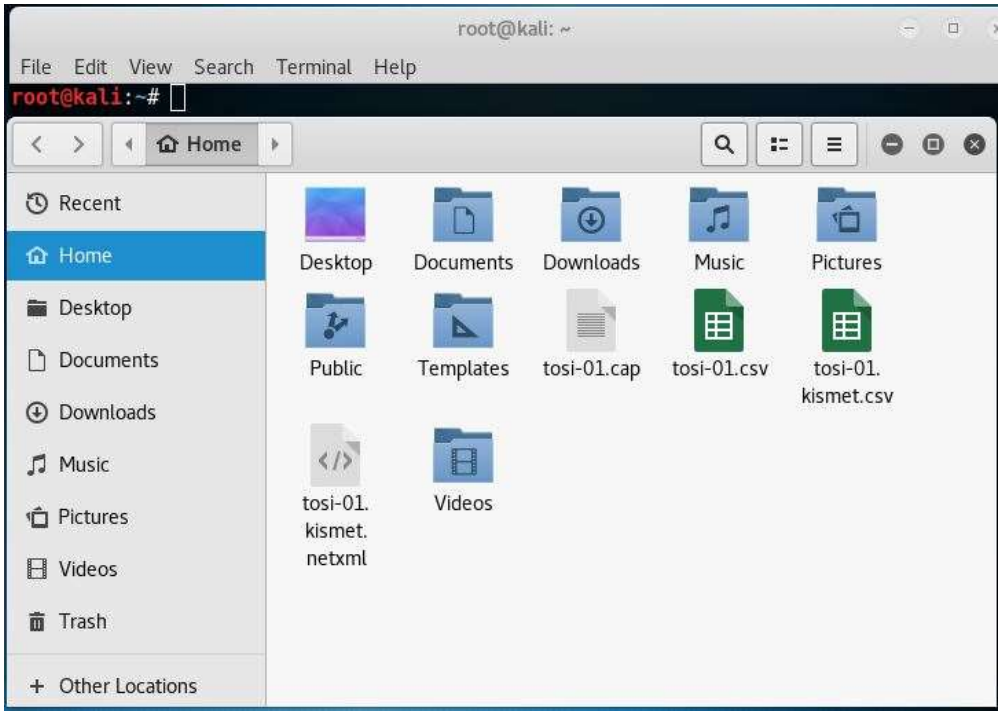


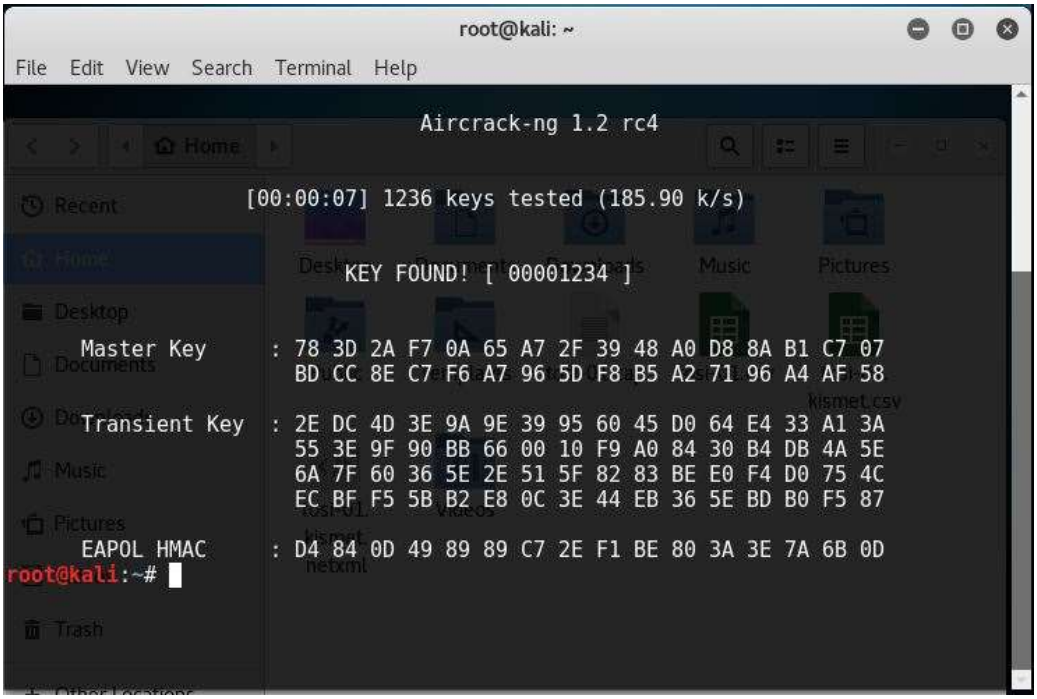
ขั้นตอนนี้ให้จะทำการใช้คำสั่ง airodump-ng -w ak -c 11 --bssid 50:46:5D:5E:78:42 wlan0 สำหรับ ดักจับ แพ็กเก็จ ด้วยวิธี Hashcat จากนั้นใช้คำสั่ง aireplay-ng -0 5 -a 50:46:5D:5E:78:42 wlan0 เพื่อทำการโจมตี อุปกรณ์ที่ใช้ในการปล่อยสัญญาณ



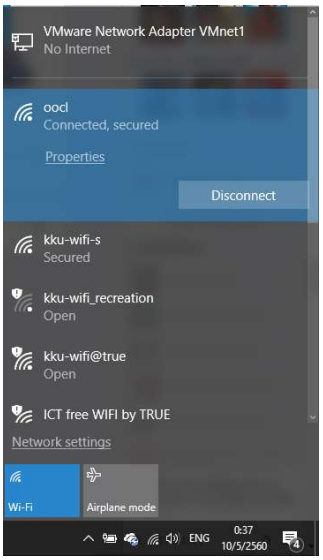


หลังจากที่ทำการโจมตีแล้วจะได้ ไฟล์ .cap ที่ได้จการดักจับแพกเกจ เพื่อนำไป เข้ารหัสด้วยวิธี Brute Force โดยใช้ คำสั่ง Script CRUNCH ในการเข้ารหัส





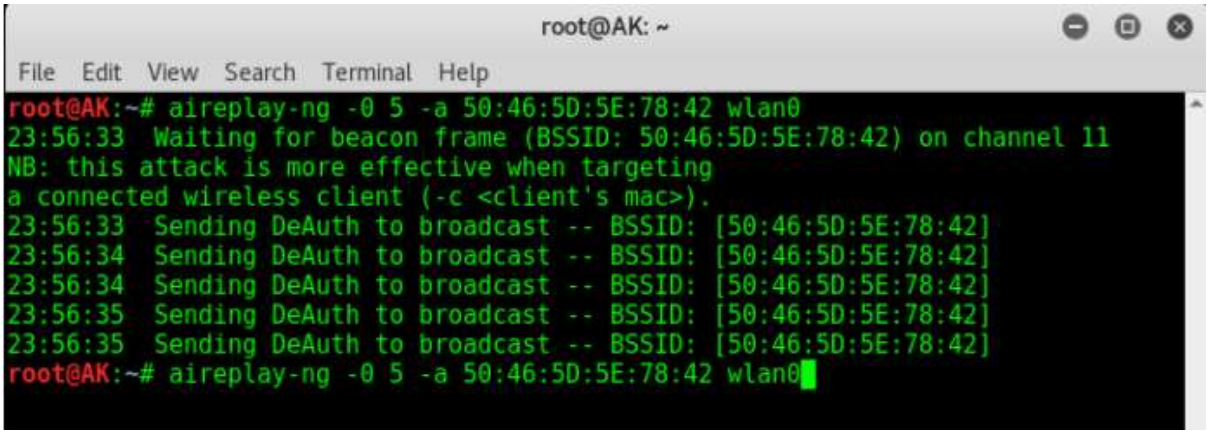
ขั้นตอนนี้คือการ เข้ารหัส ไฟล์ .cap ด้วยวิธี Brute Force โดยใช้ คำสั่ง Script CRUNCH ในการเข้ารหัส คือ crunch 8 10 0123456789 | aircrack-ng tosi.cap -w - -b 48:3C:088:19:30



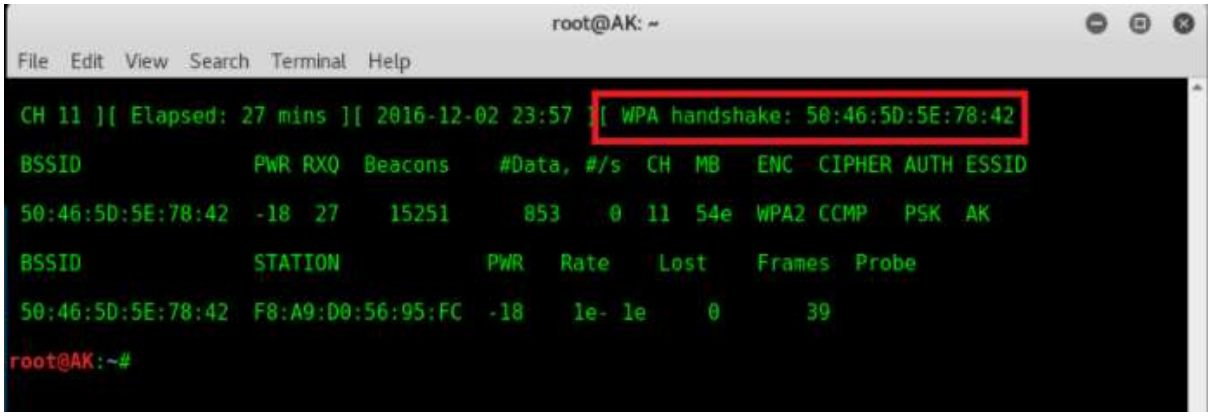
นำรหัสที่ได้จากการการ Brute Force มาทดสอบยืนยันตัวตนเข้าใช้งานเครือข่าย ว่าสามารถเข้าใช้งานเครือข่ายได้หรือไม่

บทที่ 4
ผลการดำเนินงาน

ในการดำเนินงานตามโครงงานในการทดสอบความปลอดภัยของระบบเครือข่ายไร้สาย โดยการการใช้ระบบ ทดสอบความปลอดภัย Kali Linux โดยการใช้วิธีการ Hashcat และ การเข้ารหัส ไฟล์ โดยวิธีการ Brute Force เพื่อให้ได้มาซึ่งรหัสผ่านในการเข้าใช้งานเครือข่ายไร้สาย

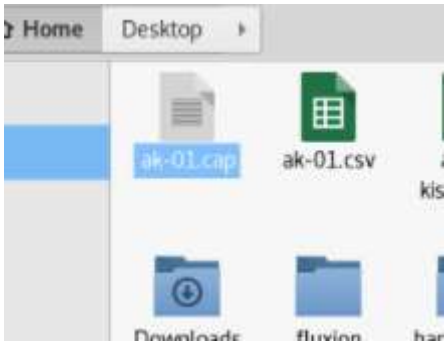


จากภาพ เป็นขั้นตอนการส่งแพกเกจ สำหรับ ส่งไปที่ ตัวเป้าหมายเพื่อ ทำการดักจับ แพกเกจ ในการเข้ารหัส ของ ผู้ที่ใช้งาน เครือข่ายไร้สายนี้อยู่

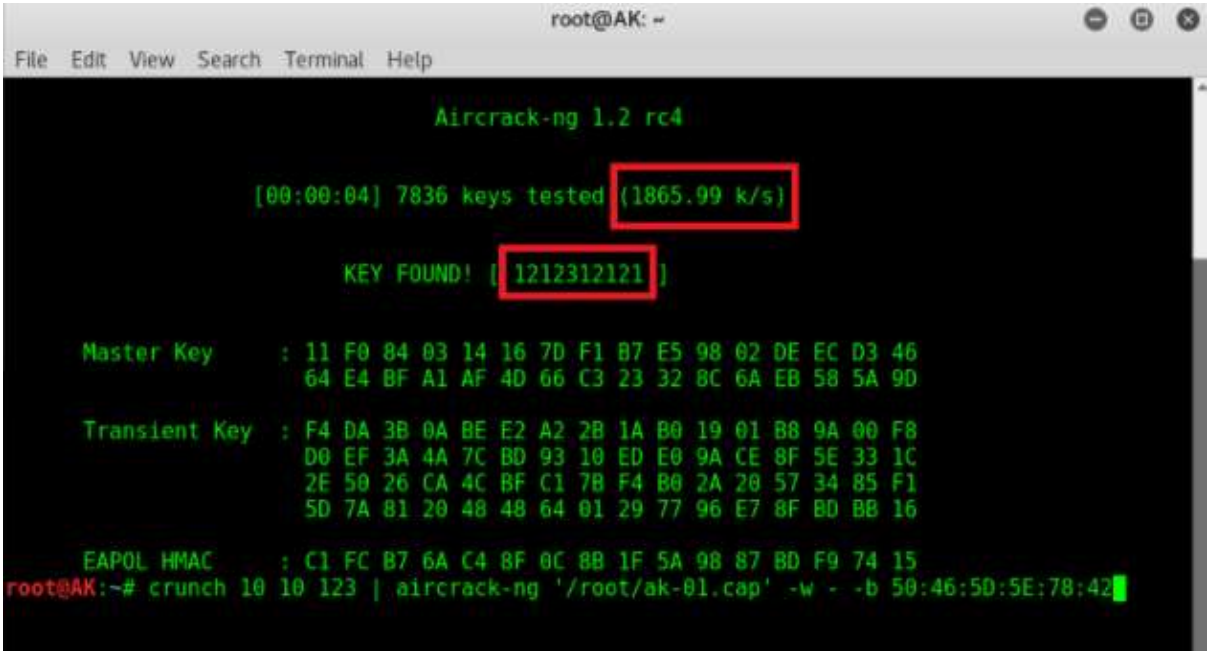


จากภาพ หลังจากที่ส่งแพกเกจ ไปและ ทำให้ ผู้ใช้งานเครือข่ายขาดเชื่อมต่อจากเครือข่าย ทำให้ต้องมีการพยายามเชื่อมต่อเครือข่ายใหม่อีกครั้ง ซึ่งตอนนี้ ระบบจะดักจับแพกเกจจาก การพยายามเข้ามา เชื่อมต่อเครือข่ายทำให้ ได้ ไฟล์ ข้อมูล .cap มา เพื่อเข้าสู่ขั้นตอนในการเข้ารหัสต่อไป

ในส่วนของขั้นตอนในการเข้ารหัส โดยการใช้วิธี Brute Force ซึ่งจะต้องนำไฟล์ .cap จากขั้นตอนข้าง ต้นมาเข้ารหัสเพื่อ ให้ได้รหัสผ่านที่ถูกต้อง



ในการเข้ารหัสไฟล์ นั้น จะต้องมีการสุ่ม ตัวอักษร ตัวเลข หรือ สัญลักษณ์ ซึ่งในบางกรณีจะต้อง ใช้เวลานานมากในการถอดรหัส ดังนั้น การตั้งรหัสผ่านของเครือข่ายไร้สายนั้น จึง ควรมีการ เลือก การตั้งรหัสผ่านที่มีความยาก จึงจะมีความปลอดภัยต่อเครื่อข่าย



จากภาพแสดงให้เห็นว่าหากสามารถเข้ารหัสไฟล์ ข้อมูล ทำให้ได้รหัสผ่านสำหรับเครือข่าย ไร้สาย

บทที่ 5
อภิปรายผลการดำเนินงาน

ในการดำเนินงานตามโครงงานในการทดสอบความปลอดภัยของระบบเครือข่ายไร้สาย โดยการการใช้ระบบ ทดสอบความปลอดภัย Kali Linux โดยการใช้วิธีการ Hashcat และ การเข้ารหัส ไฟล์ โดยวิธีการ Brute Force เพื่อให้ได้มาซึ่งรหัสผ่านในการเข้าใช้งานเครือข่ายไร้สาย

ซึ่งจากการศึกษาพบว่า ในการทดสอบความปลอดภัยของเครือข่ายไร้สาย นั้นสามารถใช้ได้ในบางกรณี ซึ่งความยากง่าย ของรหัสผ่านนั้นเป็นอีกปัจจัย ที่มีผลต่อการใช้ Kali linux อีกทั้ง ชนิดของความปลอดภัย นั้นมีผลอีกเช่นกัน ดังนั้น ในการปกป้องเครือข่ายไร้สายนั้นต้องพยายาม อัพเดทรหัสผ่าน และซอฟต์แวร์ใหม่เสมอเพื่อให้ เกิดความทันสมัยและเท่าทันในเทคโนโลยีของการป้องกันเครือข่าย

เอกสารอ้างอิง

- Nakornb. *เทคโนโลยีเครือข่ายไร้สาย* .เว็บไซต์ : http://chilchil.swu.ac.th.ปีที่ : 2551 แหล่งที่มา : http://chilchil.swu.ac.th/wiki/index.php/%E0%B9%80%E0%B8%84%E0%B8%A3%E0%B8%B7%E0%B8%AD%E0%B8%82%E0%B9% , เข้าถึงเมื่อ 4 พฤษภาคม 2560.

- Srinakharinwirot University.. *มาตรฐาน IEEE 802.11* .เว็บไซต์ : http://wise.swu.ac.th/. ปีที่ : 2001 แหล่งที่มา : http://wise.swu.ac.th/Default.aspx?tabid=3440 , เข้าถึงเมื่อ 4 พฤษภาคม 2560.

- Srinakharinwirot University.. *มาตรฐาน IEEE 802.11* .เว็บไซต์ : http://wise.swu.ac.th/. ปีที่ : 2001 แหล่งที่มา : http://wise.swu.ac.th/Default.aspx?tabid=3440 , เข้าถึงเมื่อ 4 พฤษภาคม 2560.