บทความวิจัย

ระบบตรวจจับและตอบโต้การโจมตีด้วนเทคนิคแฝดนรก

Detection and Response System Against The Evil Twin Attack

สมนึก พ่วงพรพิทักษ์, นราธิป คำควร, ศิริภัทร ดำนิน

สาขาวิทยาการคอมพิวเตอร์ คณะวิทยาการสารสนเทศ มหาวิทยาลัยมหาสารคาม

บทคัดย่อ

ระบบตรวจจับและตอบโต้การโจมตีด้วยเทคนิคแฝดนรก เป็นระบบที่สามารถตรวจจับการโจมตีเครือข่ายไร้สายภายในองค์กร และ สามารถแจ้งเตือนเมื่อตรวจพบการโจมตีเครือข่ายไร้สายผ่านช่องทาง Line Group และ Email ไปยังผู้ใช้งานเพื่อให้ทราบถึงการโจมตีได้ทันทีก่อนที่จะเกิดความเสียหาย และสามารถตอบโต้การโจมตีเบื้องต้นได้ด้วยวิธีการ de-authen เพื่อหยุดยั่งการโจมตีเบื้องต้น เพื่อดำเนินการแก้ปัญหาต่อไป ทำให้เกิดความปลอดภัยในการใช้งานเครือข่ายไร้สายภายในองค์กรมากยิ่งขึ้น

คำสำคัญ: de-authentication

1.บทนำ

ในปัจจุบันเครือข่ายอิเทอร์เน็ตมีหลักๆ อยู่ 2 ประเภท คือ 1 แบบมีสาย LAN และ 2 แบบที่ไม่มีสาย WLAN ซึ่งทั้ง 2 แบบมีความจำเป็นอย่างมากในการติดต่อสื่อสาร แต่ปัจจุบันจะเห็นได้ว่าองค์กรต่างๆ นิยมใช้งานเครือข่ายไร้สายในการติดต่อสื่อสารภายในองค์กร เนื่องจากความสะดวกสบายและมีประสิทธิภาพในการใช้งานมากกว่าเครือข่ายอินเทอร์เน็ตแบบมีสาย แต่หากกล่าวถึงด้านความปลอดภัยของเครือข่ายไร้สายแล้ว เครือข่ายไร้สายนั้นมีความเสี่ยงที่จะถูกโจมตีจากผู้ไม่ประสงค์ดีสูง การโจมตีเครือข่ายไร้สายนั้นสามารถทำได้หลายวิธี และ หนึ่งในการโจมตีที่ Hacker ยังนิยมใช้ในปัจจุบันคือ การโจมตีด้วยเทคนิค Evil Twin Attack หรือที่รู้จักกันในชื่อ Rouge Access Point โดยมีลักษณะการโจมตีคือการทำ Access Point ปลอมที่มีความเหมือนหรือคล้ายคลึงกับเป้าหมาย และ เมื่อเหยื่อทำการเชื่อมต่อกับ Access Point นั้น จะสามารถทำการดักจับข้อมูลหลายๆอย่างได้

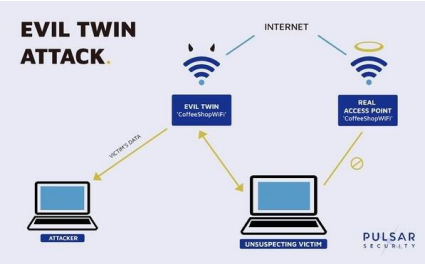
ดังนั้นผู้จัดทำจึงขอเสนอ เครื่องมือที่สามารถตรวจสอบการโจมตีของ Evil Twin attack ซึ่ง เป็นซอฟต์แวร์ที่จะสามารถค้นหาและตอบโต้ไม่ให้ Evil Twin attack นั้นสามารถใช้โจมตีหรือหลอกให้เหยื่อเข้าไปเชื่อมต่อเพื่อใช้งานและคาดหวังที่จะดักข้อมูลต่างๆของเหยื่อ โดยตัวซอฟต์แวร์จะเพิ่มความสะดวกให้ผู้ถือครองคือ จะแจ้งเตือนผ่าน Message ของ Line และ E-mail เพื่อให้ผู้ถือครองรับทราบพิกัดของ Evil Twin attack และรับมือได้ทันท่วงที

2.ทฤษฎีที่เกี่ยวข้อง

Evil Twin Attack

Evil Twin Attack [1] คือ การตั้งค่าหรือปลอมแปลงข้อมูลของ Access Point ให้เหมือนกับ Access Point ที่เป้าหมายต้องการเชื่อมต่อโดยจงใจให้มี ESSID (ชื่อของ WiFi ที่

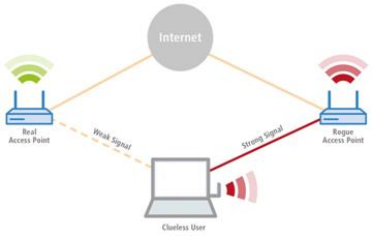
ระบุว่าเป็นของเราหรือสถานที่นั้นๆให้บริการ) เหมือนกันเช่น การตั้งชื่อ Airport WIFI แล้วนำไปติดตั้งไว้ที่สนามบิน เพื่อให้เป้าหมายทำการเชื่อมต่อสัญญาณ WiFi ที่ถูกกระจายสัญญาณออกไปใหม่ หากเป้าหมายทำการเชื่อมต่อสัญญาณ WiFi ดังกล่างโดยที่เป้าหมายไม่ทันสังเกตอาจทำให้ผู้ไม่ประสงค์ดีล้วงเอาข้อมูลไปได้



ภาพประกอบที่ 1 Evil Twin Attack

Rouge Access Point

Rogue Access Point [2] คือตัวกระจายสัญญาณ WiFi ที่ทำให้ผู้ใช้งานที่ต้องการเชื่อมต่อ Access Point จริงให้เชื่อมต่อกับ Access Point ของ Hacker แทนโดยที่ผู้ใช้งานจะไม่รู้ตัวเลยว่ามีการดักจับข้อมูลอยู่ เพราะการทำงานของ Rogue Access Point เหมือน Access Point ปกติทุกประการ ในบางครั้งบุคคลทั่วไปจะคิดว่า Evil Twin attack เป็น Rouge Access Point หากพูดถึงกระบวนการทำงานอาจจะมีส่วนที่คล้ายคลึงกันบางประการ เช่น ทำการเปิด Access Point เพื่อหลอกให้เหยื่อเข้าไปใช้งานและดักจับข้อมูลได้



ภาพประกอบที่ 2 Rouge Access Point

Air Crack

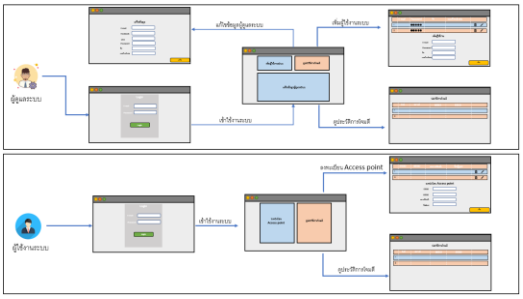
Air Crack[4] คือ Tool ที่ใช้ในการดับจับและวิเคราะห์ข้อมูลของเครือข่าย Wireless LAN สามารถใช้ในการ Crack ข้อมูลที่เข้ารหัสทั้งในรูปแบบของ WEP WPA1 และ WPA2 และใน Monitor Mode สามารถใช้ในการตรวจจับและวิเคราะห์ข้อมูลต่างๆ ของ Wireless LAN รอบๆตัวได้ โดย Tool นี้มี option หลากหลายมาก และหนึ่งใน option ที่คนส่วนมากรู้จักและใช้งานบ่อยครั้ง คือ การทำ WPA hand-shake ซึ่งจะสามารถนำไฟล์ Pcap ที่ได้จากการดักจับข้อมูลนี้ไป Crack หา Password ได้

De-authentication Attack

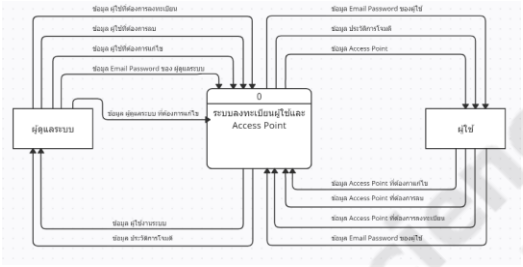
De-authentication Attack [5] คือการส่งเฟรม De-authentication packet ไปยังเครื่องที่กำลังเชื่อมต่อหรือติดต่อกับอุปกรณ์กระจายสัญญาณของเป้าหมาย เมื่อเครื่องเป้าหมายได้รับเฟรม De-authentication ซึ่งทำให้เครื่องที่ได้รับเฟรมดังกล่าวนั้นเข้าใจว่าได้รับการขอยกเลิกการเชื่อต่อหรือการไม่สามารถให้บริการได้จากอุปกรณ์กระจายสัญญาณเป้าหมาย ซึ่งทำให้เครื่องที่เชื่อมต่ออยู่กับ Access Point นั้นไม่สามารถเชื่อมต่อได้ การส่งเฟรม De-authentication นั้นยังสามารถส่งไปยัง Access Point โดยตรงได้

ซึ่งจะทำให้เครื่องที่เชื่อต่ออยู่กับ Access Point ดังกล่าวไม่สามารถเชื่อต่อกับ Access Point ได้ โดยมีตัวอย่างการใช้งานดังนี้

3.แผนการดำเนินงาน



ภาพประกอบที่ 3 ภาพรวมของระบบ



ภาพประกอบที่ 4 แผนภาพบริบทของระบบ

4.การทดสอบแอปพลิเคชัน

การทดสอบระบบโดยเป็นการทดสอบการทำงานทั้งระบบ (System Test) เพื่อทดสอบการทำงานของระบบตรวจจับและตอบโต้การโจมตีด้วยเทคนิคแฝดนรก(Detection and Response system Against The Evil Twin Attack) และ เว็บไซต์สำหรับลงทะเบียน Access Point เพื่อให้ทราบว่าระบบมีการทำงานถูกต้องหรือไม่ โดยมีการเพิ่มข้อมูล ลบข้อมูล และได้ทำแบบประเมินกับผู้ร่วมทดลองเพื่อวัดค่าความสมบูรณ์ของระบบและเว็บไซต์ว่าอยู่ในระดับใด

5.สรุปและอภิปรายข้อเสนอแนะ

5.1 สรุปผลและอภิปราย

หลังจากได้พัฒนาและทดสอบการทำงานของฟังก์ชันต่างๆ ของระบบตรวจจับและตอบโต้การโจมตีด้วยเทคนิคแฝดนรก และเว็บไซต์สำหรับลงทะเบียน พบว่าฟังก์ชันต่างๆ ทำงานได้อย่างถูกต้อง และ เพื่อให้เห็นถึงมุมมองของผู้ใช้งานจึงทำแบบประเมินความพึงพอใจในการใช้งานโดย ซึ่งการออกแบบ อยู่ในระดับดี และ การทำงานอยู่ในระดับดี

5.2 ปัญหาและอุปสรรค์ในการดำเนินงาน

จากที่ผู้พัฒนาได้ทำการเริ่มพัฒนาระบบตรวจจับและตอบโต้การโจมตีด้วยเทคนิคแฝดนรก สามารถสรุปปัญหาที่พบระหว่างการพัฒนาระบบได้ดังนี้

5.2.1 การตรวจจับสัญญาณเครือข่ายไร้สายในบริเวณรอบๆนั้นไม่สามารถตรวจจับเจอสัญญาณเครือข่ายไร้สายที่มีความยาวของชื่อสัญญาณเครือข่ายไร้สาย (ESSID) ที่มีความยาวจนเกินไป

5.2.2 ช่องสัญญาณ (Channel) ของสัญญาณเครือข่ายไร้สายมีการเปลี่ยนแปลงตลอดเวลาเนื่องจาก การค้นหาช่องสัญญาณในปัญจุปันเป็นแบบอัตโนมัติ

5.3 ข้อเสนอแนะ

เนื่องจากระบบตรวจจับและตอบโต้การโจมตีด้วยเทคนิคแฝดนรก ถูกพัฒนาขึ้นเพื่อใช้ภายในองค์กรโดยมีจุดประสงค์เพื่อความปลอยภัยในการใช้งานเครือข่ายไร้สายภายในองค์กร สามารถนำไปต่อยอดได้หลายส่วนดังนี้

5.3.1 เพิ่มฟังก์ชันการแจ้งเตือนผ่าน Facebook เพื่อให้ผู้ใช้สามารถรู้ถึงการโจมตีได้สะดวกมากยิ่งขึ้น

6.เอกสารอ้างอิง

1. P. Shrivastava, M. S. Jamal, and K. Kataoka, “EvilScout: Detection and Mitigation of Evil Twin Attack in SDN Enabled WiFi,” *IEEE Trans. Netw. Serv. Manag.*, vol. 17, no. 1, 2020, doi: 10.1109/TNSM.2020.2972774.
2. W. Wu, X. Gu, K. Dong, X. Shi, and M. Yang, “PRAPD: A novel received signal strength–based approach for practical rogue Access Point detection,” *Int. J. Distrib. Sens. Networks*, vol. 14, no. 8, 2018, doi: 10.1177/1550147718795838.
3. A. Acosta-López, E. Y. Melo-Monroy, and P. A. Linares-Murcia, “Evaluation of the WPA2-PSK wireless network security protocol using the Linset and Aircrack-ng tools,” *Rev. Fac. Ing.*, vol. 27, no. 47, 2018, doi: 10.19053/01211129.v27.n47.2018.7748.
4. A. Arora, “Preventing wireless deauthentication attacks over 802.11 Networks,” *arXiv*, 2018.