บทที่ 3
แพ็กเก็ตแคปเจอร์
Packet Capture

3.1 ความหมายแพ็กเก็ตแคปเจอร์ (Packet Capture)

คำว่า สนิฟเฟอร์ (Sniffer) นั้นเครื่องหมายการค้าซึ่งจดทะเบียนไว้โดยบริษัท Network Associates Inc. ในสหรัฐฯ เพื่อใช้ในผลิตภัณฑ์ของตนเองชื่อ Sniffer Network Analyzer ซึ่งเป็นโปรแกรมวิเคราะห์เนตเวิร์กโดยอาศัยการดักจับข้อมูลภายในเนตเวิร์ก ต่อมาคำนี้ถูกนำมาใช้เรียกอุปกรณ์ประเภทนี้ที่นำมาใช้ในการดักอ่านข้อมูลกันอย่างแพร่หลาย จนเป็นที่เข้าใจว่าสนิฟเฟอร์เป็นเครื่องมือในการดักจับข้อมูลบนเนตเวิร์ก ซึ่งถ้าหากเรียกให้ถูกต้องอุปกรณ์ประเภทนี้ควรเรียกว่า Netwire Tapping Device

แพ็กเก็ตแคปเจอร์ คืออุปกรณ์ที่ทำหน้าที่ดักจับแพ็กเก็ตที่วิ่งอยู่บนเนตเวิร์ก โดยจะทำงานร่วมกับเนตเวิร์กอินเทอร์เฟซการ์ด (Network Interface Card) ในโหมดโพรมิสคูอัส (Promiscuous-mode) โดยทำงานร่วมกันในโหมดนี้ การทำงานของเนตเวิร์กอินเทอร์เฟซการ์ดในโหมดนี้จะไม่มีการเปรียบเทียบแอดเดรสปลายทางของแพ็กเก็ตกับแอดเดรสของเนตเวิร์กอินเทอร์เฟซการ์ด นั่นคือทุกๆแพ็กเก็ตมาถึงยังเนตเวิร์กอินเทอร์เฟซการ์ด จะถูกจับแพ็กเก็ตขึ้นมาได้ทั้งหมดไม่เลือกว่าจะระบุแอดเดรสปลายทางของการ์ดเนตเวิร์กอินเทอร์เฟซอันไหน

แพ็กเก็ตแคปเจอร์ จะถูกใช้ในการเฝ้ากูการจราจรในเครือข่าย ให้มีประสิทธิภาพและแก้ไขปัญหาต่างๆ ที่เกิดจากการทำงาน ผิดพลาดของเครือข่าย และยังเป็นเครื่องมือในการศึกษา การทำงานของโพรโตคอลร่วมถึงการดูแลความปลอดภัยของระบบ

3.2 องค์ประกอบของแพ็กเก็ตแคปเจอร์

3.2.1 ฮาร์ดแวร์ (Hardware) หมายถึง อุปกรณ์อิเล็กทรอนิกส์ที่สามารถดักอ่านสัญญาณจากเนตเวิร์กเข้ามาได้ และสามารถนำสัญญาณที่ให้ส่งต่อไปประมวลผลออกมาเป็นข้อมูลทางคอมพิวเตอร์ได้ หน้าที่หลัก คือ จัดการกับการรับข้อมูลในระดับฟิสิคัล (Physical) อุปกรณ์นี้โดยทั่วไปก็คือเนตเวิร์กอแดปเตอร์

3.2.2 ไดรเวอร์ (Driver) เป็นโปรแกรมระดับล่างที่ควบคุมการดักจับข้อมูลของฮาร์ดแวร์ไปเก็บเป็นข้อมูลดิบรอการประมวลผลในลำดับถัดไป

3.2.3 บัฟเฟอร์ (Buffer) เป็นหน่วยความจำที่ใช้พักข้อมูลจากการดักมาได้ของ Driver โดยจะทำงานการจัดเก็บเพียงชั่วคราว และหมุนเวียนข้อมูลเข้ามาเสมอ กลไกการนำข้อมูลจากไดรเวอร์มาเก็บในบัฟเฟอร์ จะเป็นตัวบอกสถานะของการดักข้อมูลได้ความเร็วสูงสุดเท่าใด หากกระบวนการนำข้อมูลไปเก็บเป็นไปอย่างล่าช้า ย่อมทำให้แพ็กเก็ตแคปเจอร์ ไม่สามารถดักข้อมูลที่อยู่บนเนตเวิร์กได้ทันและต้องปล่อยข้อมูลนั้นทิ้งไป

3.2.4 ซอฟต์แวร์ (Software) เพื่อทำหน้าที่จัดการข้อมูลที่ได้เข้าโดยการประมวลผลตามวัตถุประสงค์ของการดักอ่านข้อมูลนั้น เนื่องจากข้อมูลดิบที่ดักได้นั้นจะเป็นข้อมูลในระดับต่ำ คือ เนตเวิร์ก

อินเทอร์เฟซเลเยอร์ (Network Interface Layer) ซึ่งจะมีข้อมูลที่ยังไม่ผ่านการมัลติเพล็กซ์และการจัดรูปแบบให้เข้าใจได้ ส่วนที่ได้จะเป็นข้อมูลเลขฐานสอง 0 กับ 1 จำนวนมหาศาลที่ต้องนำมาแปลความหมาย และอีกหน้าที่หนึ่งคือ ข้อมูลที่ดักได้นั้น เป็นการสื่อสารของทุกโฮสต์ที่อยู่ภายในเนตเวิร์กนั้นร่วมกันอยู่อย่างไม่เป็นระเบียบและไม่มีการแยกแยะว่าเป็นการสื่อสารเรื่องอะไร ระหว่างโฮสต์ใดกับโฮสต์ใด การที่จะแปลความหมายข้อมูลนี้ได้ก็จำเป็นต้องมีโปรแกรมสำหรับทำหน้าที่แปลความหมายของข้อมูลให้อยู่ในรูปแบบที่สามารถเข้าใจได้มากขึ้น นั่นคือการทำหน้าที่คล้ายกับดีมัลติเพล็กซ์ของข้อมูลทุกๆโฮสต์โดยไม่สนใจว่าเป็นข้อมูลของโฮสต์ใด

หลังจากข้อมูลผ่านการดีมัลติเพล็กซ์แล้วก็จะอยู่ในรูปที่สามารถเข้าใจได้ง่ายขึ้น แต่จะเข้าใจมากน้อยขึ้นอยู่กับความสามารถในการดีมัลติเพล็กซ์ของโปรแกรม หากการดีมัลติเพล็กซ์ได้จนถึงโพรโตคอลเลเยอร์ที่สูง รวมทั้งมีการแยกแยะหมวดหมู่ของการสื่อสารของแต่ละโฮสต์ก็จะเห็นความต่อเนื่องของการสื่อสารได้ดีขึ้น

ในส่วนการจัดเก็บข้อมูลดิบที่ดักมาได้ โปรแกรมแคปเจอร์ส่วนใหญ่จะทำการเก็บข้อมูลดิบที่ดักมาได้ไว้ในฐานข้อมูลเพื่อให้สามารถนำกลับมาวิเคราะห์ในภายหลังได้ เพราะในการแคปเจอร์จะต้องคอยดักจับข้อมูลอยู่ตลอดเวลา หากทำการดีมัลติเพล็กซ์ทันทีที่ได้รับข้อมูลในแบบเรียลไทม์อาจทำให้ประสิทธิภาพของแคปเจอร์ลดต่ำลง และเนื่องจากการสื่อสารข้อมูลจะต้องอาศัยความต่อเนื่องของการเชื่อมโยงกันของหลายๆแพ็กเก็ต ประกอบการดีมัลติเพล็กซ์ส่วนใหญ่จะสามารถทำได้ก็ต่อเมื่อข้อมูลได้รับมาครบถ้วนสมบูรณ์ทั้งหมดแล้วเท่านั้น

3.3 การทำงานของแพ็กเก็ตแคปเจอร์

การทำงานของแพ็กเก็ตแคปเจอร์ อาศัยหลักการของโพรโตคอลอีเทอร์เนต ที่ใช้การกระจายของข้อมูลไปยังทุกโฮสต์ที่อยู่ในเนตเวิร์กและอาศัยโฮสต์แต่ละตัวทำหน้าที่จำแนกการสื่อสารของตนเอง นั่นหมายความว่าข้อมูลทุกแพ็กเก็ตที่ใช้สื่อสารกันได้ถูกส่งไปยังทุกโฮสต์ ซึ่งจะได้รับพร้อมกันแล้วเหมือนกัน เพียงแต่การที่จะสื่อสารกันได้อย่างถูกต้องนั้นโฮสต์แต่ละตัวจะต้องมีกระบวนการที่สามารถรู้ได้ว่าข้อมูลแพ็กเก็ตใดเป็นของตนเอง และข้อมูลแพ็กเก็ตใดมิใช่ของตัวเอง ทุกๆแพ็กเก็ตที่กระจายลงบนเนตเวิร์กนั้น จะมีหมายเลข ระบุชัดเจน คือ แมคแอดเดรส (Mac Address) หรือเรียกอีกอย่างหนึ่งว่า อีเทอร์เนต (Ethernet Address) ซึ่งจะเป็นสิ่งที่บอกว่าแพ็กเก็ตมาจากฮาร์ดแวร์ใดในเนตเวิร์ก ทำให้สามารถระบุได้ว่าส่งมาจากโฮสต์ใด

แมคแอดเดรส จะเป็นหมายเลขเฉพาะฮาร์ดแวร์ทุกชนิดที่ใช้สื่อสารโดยโพรโตคอลอีเทอร์เนต และในทางทฤษฎีแล้วฮาร์ดแวร์ทุกชนิดจะไม่มีแมคแอดเดรสซ้ำกัน โดยทั่วไปแมคแอดเดรสจะกำหนดตายตัวอยู่ในรอม (Rom) ของฮาร์ดแวร์และไม่สามารถเปลี่ยนแปลงได้ด้วยซอฟต์แวร์

การใช้งานของฮาร์ดแวร์จะต้องควบคู่กับไดร์เวอร์ของฮาร์ดแวร์นั้นๆโดยปกติแล้วไดรเวอร์จะถูกกำหนดให้ปฏิบัติตามโพรโตคอลอย่างเข้มงวดคือ

- ให้รับข้อมูลที่มีแมคแอดเดรสเป็นของตนเองเท่านั้น (ห้ามอ่านข้อมูลของผู้อื่น)
- ให้ส่งข้อมูลโดยใช้แมคแอดเดรสของตนเองเท่านั้น (ห้ามปลอมเป็นผู้อื่น)

ดังนั้นหากใช้ไดรเวอร์ตามปกติที่มากับฮาร์ดแวร์แล้วเครื่องคอมพิวเตอร์ก็จะทำงานอยู่ในระเบียบเรียบร้อย และไม่สามารถวุ่นวายกับข้อมูลของผู้อื่นได้ แพ็กเก็ตแคปเจอร์จึงจำเป็นที่ต้องใช้โหมดการทำงานพิเศษที่อนุญาตให้รับข้อมูลที่แมคแอดเดรสไม่ใช่ของตนได้โหมดนั้นเรียกว่า พรอมิสคิอัสโหมด (Promiscuous Mode) ที่ทำให้ฮาร์ดแวร์สามารถรับข้อมูลดิบทั้งหมดบนเนตเวิร์กเข้ามาได้ โดยไม่สนใจว่าข้อมูลทั้งหมดเป็นของใคร ส่งให้ใคร

จากรูปที่ 3.1 ในเนตเวิร์กมีโฮสต์อยู่ 4 ตัว ต่อรวมกันเป็นเนตเวิร์กโดยใช้ฮับ (Hub) ร่วมกันและมีโฮสต์ตัวหนึ่งรันโปรแกรม ที่ทำหน้าที่เป็นโปรแกรมแคปเจอร์เพื่อดักจับข้อมูลที่เสียบต่อรวมกับฮับนั้น จากรูปแสดงให้เห็นการกระจายข้อมูลของโฮสต์ A ต้องการส่งให้โฮสต์ B ข้อมูลได้กระจายไปยังทุกโฮสต์ที่ต่ออยู่บนฮับ รวมถึงแพ็กเก็ตแคปเจอร์ด้วย

โฮสต์ B เมื่อได้รับข้อมูลก็จะตรวจแมคแอดเดรส ถ้าพบว่าเป็นข้อมูลที่ถูกส่งมาหาตนเองก็จะทำการอ่านและส่งต่อให้ระบบปฏิบัติการประมวลผล

โฮสต์ C และ โฮสต์ D โฮสต์ทั้งสองซึ่งมีเนตเวิร์กอแดปเตอร์ทำงานอยู่ในโหมดปกติ เมื่อได้ทำการตรวจสอบแล้วเห็นว่าไม่ใช่ข้อมูลของตนเอง ก็จะไม่สนใจข้อมูลนั้น

แพ็กเก็ตแคปเจอร์ สำหรับแพ็กเก็ตแคปเจอร์นั้นมีเนตเวิร์กอแดปเตอร์ที่ทำงานอยู่ในโพมิคูอัสโหมด นั่นคือไม่สนใจว่าข้อมูลที่เข้ามาเป็นของใคร แพ็กเก็ตแคปเจอร์จะรับข้อมูลทั้งหมดแล้วนำไปเก็บในบัฟเฟอร์และฐานข้อมูล เพื่อนำไปประมวลผลเพื่อหาข้อมูลที่มี ประโยชน์ภายหลัง

จากเนตเวิร์กในภาพนั้นมีแพ็กเก็ตแคปเจอร์ถูกติดตั้งในตำแหน่งดังกล่าว ก็จะทำให้ข้อมูลทั้งหมดที่โฮสต์ทั้ง 4 สื่อสารกันโดยผ่านฮับที่ใช้งานร่วมกัน ไม่ว่าข้อมูลใดจะปรากฏที่ฮับก็สามารถถูกดักอ่านได้โดยแพ็กเก็ตแคปเจอร์ทันที

3.4 ประโยชน์จากแพ็กเก็ตแคปเจอร์

3.4.1 วิเคราะห์ระบบเครือข่าย (Network Analyzer) การที่แพ็กเก็ตแคปเจอร์สามารถดักข้อมูลทั้งหมดที่อยู่บนเนตเวิร์กได้ ทำให้เราสามารถนำข้อมูลดังกล่าวมาทำการแระมวลผลวิเคราะห์คุณสมบัติต่างๆของเนตเวิร์กได้หลายแง่มุม ไม่ว่าการกระจายการใช้งานของโพรโตคอลต่างๆ เช่น เอชทีทีพี (HTTP) , เอสเอ็มทีพี (SMTP) , เอฟทีพี (FTP) เพื่อจะได้ทราบว่ามีการใช้เนตเวิร์กเพื่อการใด มากน้อยเพียงใด จะทำให้สามารถจัดการเนตเวิร์กได้อย่างเหมาะสม หรือในด้านการใช้งานเนตเวิร์กตามช่วงเวลาต่างๆเวลาใดที่มีผู้ใช้มาก เวลาใดที่มีผู้ใช้น้อย ผู้ใช้คนใดใช้แบนด์วิดธ์ไปในทางที่เป็นประโยชน์หรือไม่

3.4.2 เครื่องมือตรวจสอบเครือข่าย (Network Debugging Tools) ในบางครั้งการหาสาเหตุความผิดปกติของแอพพลิเคชั่นต่างๆ จำเป็นที่ต้องสืบค้นลึกลงไปถึงเนื้อข้อมูลที่รับส่งกันจริงๆบนเนตเวิร์กเพื่อหาว่าเหตุใดการทำงานของแอพพลิเคชั่นจึงไม่สามารถทำงานได้ตามปกติ การได้เห็นข้อมูลที่ส่งกันจริงทำให้การวิเคราะห์และแก้ไขปัญหาสามารถดำเนินการได้อย่างรวดเร็วและตรงต่อปัญหามากขึ้น โดยเฉพาะกรณีที่มีการใช้เครื่องมือในระดับเนตเวิร์กมาเกี่ยวข้อง เช่น มีการส่งข้อมูลผ่านไฟร์วอลแล้วมีปัญหา หรือการทดสอบ ACL (Access Control List) ของเราเตอร์ เป็นต้น

3.4.3 ตรวจจับแพ็กเก็ต (Packet Monitoring) การศึกษาเทคนิคของโพรโตคอลในระดับเนตเวิร์กจำเป็นต้องเห็นข้อมูลที่สื่อสารกันอยู่จึงจะสามารถเข้าใจได้และเห็นภาพจริง แพ็กเก็ตมอนิเตอร์ริ่งจะเป็นเครื่องมือที่นำแพ็กเก็ตมาแสดงให้เห็นในรูปแบบต่างๆได้

3.4.4 ระบบตรวจจับผู้บุกรุก (Intrusion Detection System) ระบบตรวจจับผู้บุกรุกก็มีพื้นฐานมาจากการดักอ่านข้อมูล เพียงแต่เป็นการประยุกต์การวิเคราะห์รูปแบบการบุกรุกเข้ากับการดักอ่านข้อมูลบนเนตเวิร์กแบบเรียลไทม์ ทำให้สามารถทราบว่ามีกิจกรรมใดบนเนตเวิร์กที่มีแนวโน้มว่าจะเป็นการบุกรุกหรือทำอันตรายต่อผู้อื่น