พ.อ.ดร. ปรัชญา เฉลิมวัฒน์
กองวิชาวิศวกรรมไฟฟ้า
ส่วนการศึกษา โรงเรียนนายร้อยพระจุลจอมเกล้า

ไวร์ชาร์คสนิฟเฟอร์กับสงครามสารสนเทศเชิงรุก

WireShark Sniffer in Offensive Information Warfare

บทคัดย่อ

ในการปฏิบัติการสงครามสารสนเทศเชิงรุก มีความจำเป็นต้องทำการดักรับหรือดักฟังข้อมูลของฝ่ายตรงข้าม เพื่อนำมาวิเคราะห์ ตรวจสอบถอดรหัส หรือโจมตีการเข้าถึงระบบด้วยเครื่องมือทางเทคโนโลยีสารสนเทศ บทความนี้นำเสนอกรณีศึกษาการนำโปรแกรมไวร์ชาร์คซึ่งเป็นสนิฟเฟอร์หรือเครื่องมือดักจับข้อมูลบนระบบเครือข่ายอินเทอร์เน็ตที่มีประสิทธิภาพ โดยนำข้อมูลตัวอย่างการดักจับแพ็คเก็ตมาวิเคราะห์ ยกตัวอย่างการเฝ้าระวัง การค้นหารหัสผ่านบนระบบเครือข่าย ผลการศึกษาพบว่าไวร์ชาร์คสามารถนำมาใช้งานในสงครามสารสนเทศเชิงรุกได้เป็นอย่างดี

คำหลัก : สงครามสารสนเทศเชิงรุก โปรแกรมสนิฟเฟอร์ ไวร์ชาร์ค

Abstract

Offensive Information Warfare (OIW) involves in capturing data packets from opponent hosts connected to public network. The captured information will be used for analyzing, testing, decoding, or attacking opponent hosts. This paper describes a case study of applying one of the sniffers called WireShark to capture packets form the simulated network. It also explains the fundamental of installing WireShark and how to use it in OIW. Experimental results show the applicability of WireShark in capturing data necessary for operation in OIW.

Key words : Information Warfare, packet sniffer, WireShark

1. บทนำ

สงครามสารสนเทศ (Information Warfare) หรือในทางทหารเรียกว่า ปฏิบัติการข้อมูลข่าวสาร (Information Operation) เป็นอีกมิติของการทำสงครามซึ่งมีผลทำให้มีความได้เปรียบต่อปฏิบัติการไม่ว่าจะเป็นทางการทหาร การเมือง เศรษฐกิจ หรือผลทางด้านสังคม (2) ไวร์ชาร์ค (WireShark) เป็นโปรแกรมประเภทสนิฟเฟอร์ที่ใช้ในการวิเคราะห์ระบบเครือข่าย ด้วยการดักจับแพ็คเก็ตที่อาจมีข้อมูลสำคัญ (3) ไวร์ชาร์คพัฒนา มาจากพื้นฐานของโปรแกรมสนิฟเฟอร์ที่มีชื่อเสียงคือ Ethereal ซึ่งใช้ไลบรารี่ GTK+ ในการสร้างส่วนติดต่อผู้ใช้งานในโหมดกราฟิก และไลบรารี่ libpcap ในการดักจับและการกรองแพ็คเก็ต โปรแกรมไวร์ชาร์คที่รันในโหมดตัวอักษรเรียกว่า Tshark ซึ่งทำงานในลักษณะเดียวกันกับ tcpdump หรือ snoop ซึ่งสามารถใช้ในการจำแนก, ดักจับการอ่าน/เขียนไฟล์ และการกรองแพ็คเก็ต

การดักจับแพ็คเก็ตเป็นการกระทำที่ผิดกฎหมาย หากมิได้รับอนุญาตให้ปฏิบัติ เนื่องจากเป็นการละเมิดสิทธิของการรับ/ส่งข้อมูลผ่านระบบเครือข่าย (พระราชบัญญัติว่าด้วยการกระทำความผิดที่เกี่ยวกับคอมพิวเตอร์ 2550) รายละเอียดเพิ่มเติมของการใช้งานไวร์ชาร์คสามารถดูได้จาก (1)

2. การติดตั้งไวร์ชาร์ค

ในส่วนนี้จะกล่าวถึงการติดตั้งไวร์ชาร์คบน Ubuntu หรือลินุกซ์ทะเล 7 อย่างไรก็ตาม โปรแกรมไวร์ชาร์คสามารถคอมไพล์และรันได้ในระบบอื่นๆ เช่น Linux (เวอร์ชั่น 2.0 ขึ้นไป), Solaris, FreeBSD, NetBSD, OpenBSD, Mac OS X, HP-UX, Irix, AIX, หรือ Win32 (วินโดวส์ 98, NT, 2000, และ XP) เป็นต้น รายละเอียดการติดตั้งจากซอร์สโค้ดทั้งหมดอยู่ในไฟล์ INSTALL ในไดเร็กทอรี่ของซอร์สโค้ด และมีคำแนะนำบางส่วนอยู่ในไฟล์ README.<OS> ในเอกสารนี้จะกล่าวถึงเฉพาะการติดตั้งจากไบนารี่ที่คอมไพล์มาแล้วด้วยการใช้คำสั่ง apt-get บนระบบปฏิบัติการ Ubuntu

2.1 การติดตั้งบน Ubuntu หรือลินุกซ์ทะเล

การติดตั้งบน Ubuntu หรือ ลินุกซ์ทะเล นั้นสามารถติดตั้งได้จากไบนารี่ที่มีพร้อมให้สำหรับติดตั้งด้วย apt-get ข้อมูลพื้นฐานสำหรับการติดตั้งมีดังนี้

- ลินุกซ์ทะเล TLE 7.0 เคอร์เนิ่ลเวอร์ชั่น 2.6.17-11
- มีการเชื่อมต่อกับอินเทอร์เน็ต และตั้งค่า /etc/apt/source.list ถูกต้อง เพื่อให้สามารถดาวน์โหลดไฟล์ที่เหมาะสม และเป็นเวอร์ชั่นล่าสุด
- ใช้โปรแกรม wireShark 0.99.3a
- คอมไพล์ด้วย GTK+ 2.10.4, GLib 2.12.3, โดยใช้ libpcap 0.9.4, กับ libz 1.2.3, และ libpcre 6.4, โดยไม่ใช้ UCD-SNMP หรือ Net-SNMP และ ไม่ใช้ตัวเลือกค่า Lua
- ต้องมีการแก้ไขไลบรารี่ด้วยการแพ็ทช์ (patch) Shared Object libdatrie-0.1.1

ในการติดตั้งให้เริ่มต้นติดตั้งไวร์ชาร์คด้วยการใช้คำสั่ง

```
sudo apt-get install wireShark
```

เมื่อติดตั้งเสร็จให้ทดลองรันด้วยคำสั่งในคอมแมนด์ไลน์ หรือจากเมนูของระบบวินโดวส์

```
sudo wireshark -i eth0
```

โปรแกรมจะพยายามเริ่มการทำงานด้วยการแสดงโลโก้ของไวร์ชาร์คแล้วหยุดทำงานพร้อมทั้งรายงานข้อผิดพลาดในการรันว่า Segmentation Fault และโปรแกรมจะหยุดทำงาน (เฉพาะในระบบปฏิบัติการ Ubuntu และลินุกซ์ทะเล) ให้ทำการแก้ไขตามขั้นตอนในบทต่อไป

2.2 การแก้ไขปัญหา Segmentation Fault

โปรแกรมไวร์ชาร์คใช้ไลบรารี่แบบไดนามิค (Shared object) ของ Libdatrie[1] ซึ่งมีรายงานว่ามีปัญหาในการใช้ไวร์ชาร์คบน Ubuntu และลินุกซ์ทะเล 7 (ซึ่งพัฒนามาจากพื้นฐานของ Debian เช่นเดียวกัน) ส่วนหนึ่งของวิธีการแก้ไขได้คำแนะนำจากเว็บไซต์[2] ซึ่งไม่ได้ให้คำอธิบายการแก้ไขในแต่ละขั้นตอนที่ผู้ใช้ทั่วไปจะสามารถปฏิบัติได้ ดังนั้นผู้เขียนจึงได้ทดลองและแก้ไขให้โปรแกรมสามารถทำงานได้ตามรายละเอียดดังนี้

- ดาวน์โหลดซอร์สโค้ดของ Libdatrie จากเว็บไซต์ของ Debian
- ดาวน์โหลดแพ็ทช์สำหรับแก้ไขจากเว็บไซต์ http://research.crma.ac.th/2549/images/1/15/Patch
- ทำการแพ็ทช์ (แก้ไขซอร์สโค้ด) patch -p0 < patch
- คอมไพล์ libdatrie ใหม่
- เปลี่ยนไฟล์ /usr/lib/libdatrie.so.0.0.0 ให้เป็นไฟล์ที่คอมไพล์ใหม่ด้วยคำสั่ง cp datrie/.libs/libdatrie.so.0.0.0 /usr/lib

จากนั้นจึงจะสามารถใช้งานไวร์ชาร์ค ได้ตามปกติดังแสดงในรูปที่ 1

2.3 การใช้งานกับโปรโตคอล IPv6

ระบบปฏิบัติการที่สนับสนุนโปรโตคอล IPv6 ไวร์ชาร์คจะพยายามค้นหาชื่อโฮสต์จากข้อมูลในแพ็คเก็ต ของ IPv6 ด้วยวิธี Reverse Name Resolution หากไม่ต้อง การให้ไวร์ชาร์คทำเช่นนั้นให้รันด้วยตัวเลือก "-n" เพื่อปิดการทำงานของ Name Resolution รวมถึงการแปลง MAC แอดเดรส และ TCP/UDP/SMTP พอร์ตให้เป็นชื่อ หรือใช้ตัวเลือก "-N mt" เพื่อปิดการทำงานของ name resolution สำหรับทุกเลเยอร์แอดเดรสของ IPv4, IPv6, และ IPX หากต้องการให้เป็นค่าปริยายให้เปิดไดอะล็อกของ "Preferences" ในเมนู "Edit" เลือก "Name resolution" แล้วปิดการทำงานของตัวเลือกที่ต้องการ จากนั้นให้คลิก "Save" แล้วคลิก "Ok" หากต้องการคอมไพล์ไวร์ชาร์คโดยไม่ต้องการการทำงานกับแพ็คเก็ต IPv6 ให้ใช้ตัวเลือก "--disable-ipv6" เมื่อรันโปรแกรม "./configure" ก่อนที่จะคอมไพล์ (ไวร์ชาร์คยังสามารถเห็นแพ็คเก็ตของ IPv6 แต่จะแสดงเป็นแอดเดรสแทนชื่อ)

3. การใช้งาน

3.1 การใช้งานบน Linux

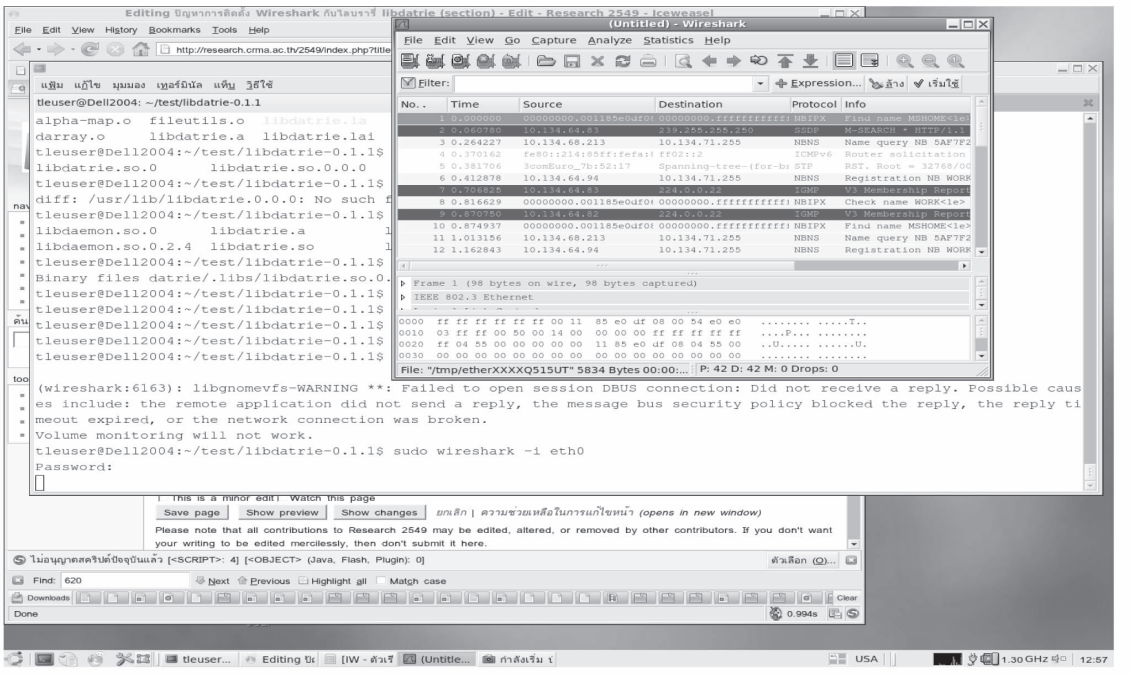
ในการดักจับแพ็คเก็ตด้วยไวร์ชาร์ค, tcpdump หรือโปรแกรมอื่นที่ใช้ไลบรารี่ของ libpcap ในระบบปฏิบัติการลินุกซ์ (Linux) โปรโตคอลของแพ็คเก็ตต้องได้รับ การสนับสนุนจากเคอร์เนิ่ลด้วย หากไม่มีการสนับสนุนดังกล่าวจะเกิดข้อความดังนี้

modprobe: can't locate module net-pf-17 in "/var/adm/messages", or may get messages such as socket: Address family not supported by protocol

จากโปรแกรมประยุกต์ที่ใช้ไลบรารี่ของ Libpcap ในกรณีนี้ผู้ใช้ต้องคอมไพล์เคอร์เนิ่ลใหม่เพื่อให้มีตัวเลือก CONFIG_PACKET สำหรับโปรโตคอลแพ็คเก็ตซึ่งใช้ สำหรับโปรแกรมประยุกต์เพื่อติดต่อโดยตรงกับอุปกรณ์เครือข่ายโดยไม่มีเน็ตเวอร์คโปรโตคอลใดเป็นตัวเชื่อม

[1] http://pclab.nectec.or.th/wiki/index.php/OLPC\THAILAND\Developer\Forums

[2] http://www.neutron.in.th/node/42



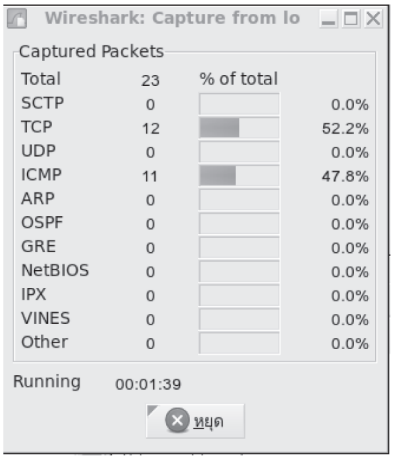
รูปที่ 1 ภาพหน้าจอการใช้งานโปรแกรมไวร์ชาร์ค

การส่งข้อมูลของแพ็คเก็ตจากเคอร์เนิ่ลไปยังโปรแกรม ใช้ทรัพยากรในการคำนวณของซีพียูค่อนข้างสูง ดังนั้นการกรองแพ็คเก็ตโดยเคอร์เนิ่ลก่อนได้ จะเป็นการช่วยลดเวลาที่ต้องสูญเสียไป (แต่ถ้าไม่มีการใช้การกรอง ประสิทธิภาพของการส่งข้อมูลแพ็คเก็ตจะมีค่าเท่ากันในทั้งสองกรณี)

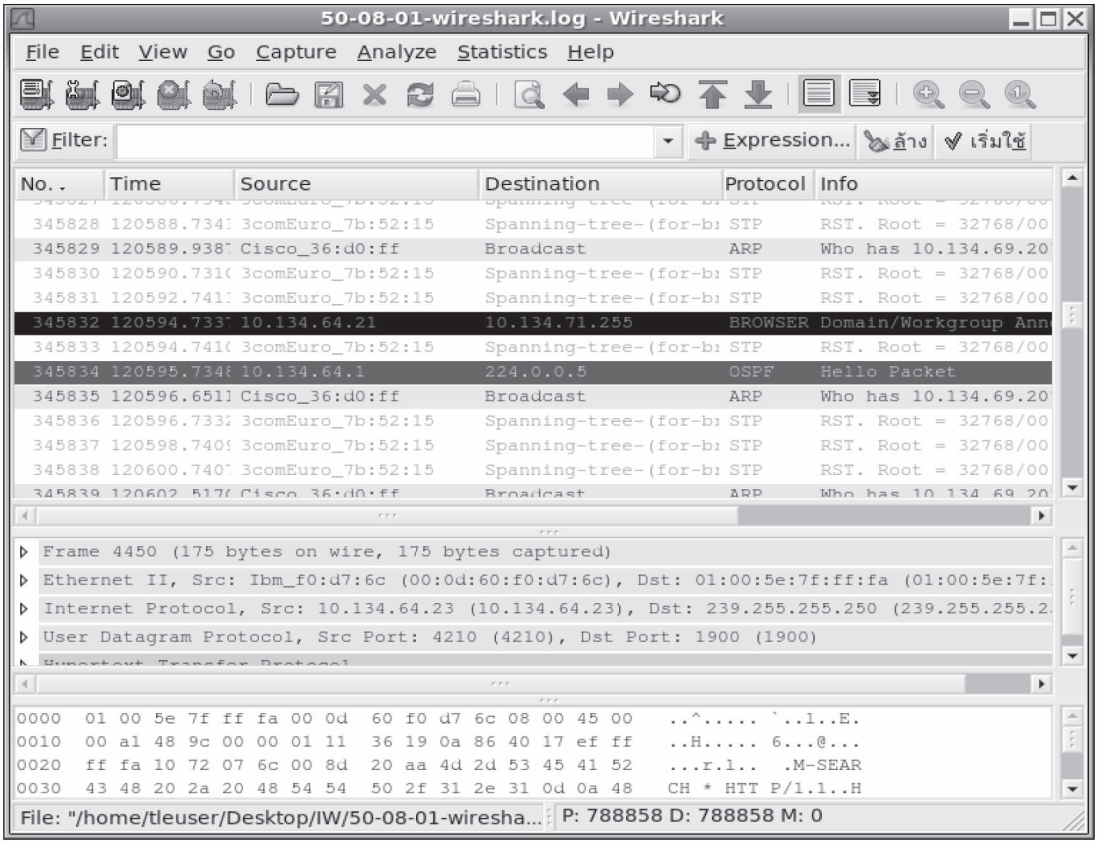
3.2 การใช้งานทั่วไป

รูปที่ 2 แสดงการทำงานเมื่อเริ่มสั่งให้ดักจับแพ็คเก็ต จากอุปกรณ์เครือข่ายที่กำหนดซึ่งอาจเป็น lo, eth0, eth1 เป็นต้น หรือทั้งหมดก็ได้ ผู้ใช้งานอาจรอให้ไวร์ชาร์คสามารถดักจับแพ็คเก็ตได้จำนวนหนึ่งเพื่อให้สามารถนำข้อมูลมาวิเคราะห์ได้ เมื่อถึงเวลาที่ต้องการแล้วให้กดปุ่ม “หยุด” ไวร์ชาร์คจะปิดหน้าต่างเล็ก แล้วกลับไปสู่หน้าต่างหลักดังแสดงในรูปที่ 2

รูปที่ 3 แสดงการแสดงผลการดักจับของไวร์ชาร์ค ซึ่งจะแสดงจำนวน เวลา ต้นทาง ปลายทาง โปรโตคอล และข้อมูลเพิ่มเติมของแต่ละแพ็คเก็ต เมื่อคลิกไปที่แพ็คเก็ตใดๆ ไวร์ชาร์คจะแสดงข้อมูลที่อยู่ในแพ็คเก็ตนั้นในส่วนล่างของหน้าต่างในรูปแบบเลขฐานสิบหกและรหัสแอสกี้ (ซึ่งอาจใช้ดักจับรหัสผ่านที่ไม่ได้ถูกเข้ารหัสได้)



รูปที่ 2 โปรแกรมไวร์ชาร์คเริ่มดักจับแพ็คเก็ตสำหรับเน็ตเวอร์คอินเทอร์เฟสที่เลือก



รูปที่ 3 โปรแกรมไวร์ชาร์คแสดงผลของแพ็คเก็ตที่ดักจับได้หลังจากสั่งให้หยุดดักจับ

ในการดักจับแพ็คเก็ตจากระบบเครือข่าย ต้องรันไวร์ชาร์คในฐานะเป็น root ของระบบคอมพิวเตอร์ที่ใช้งาน หรือต้องมีสิทธิในการควบคุมอุปกรณ์ระบบเครือข่ายที่จะใช้ (ใน Ubuntu จะใช้คำสั่ง sudo รันแทน root โดยผู้ใช้ต้องได้รับสิทธิให้อยู่ในกลุ่มที่สามารถควบคุมอุปกรณ์เครือข่ายได้) ผู้เขียนไม่แนะนำให้เซ็ตไวร์ชาร์คเป็นโหมด setuid root เนื่องจากโปรแกรมยังไม่เสถียรพอ และยังมีช่องโหว่ด้านความปลอดภัยอยู่

4. การดักฟังโฮสต์เป้าหมาย

ในการใช้งานโดยทั่วไป หากไม่ระบุรายละเอียดการทำงาน ไวร์ชาร์คจะดักจับแพ็คเก็ตทั้งหมดที่ผ่านมายังระบบเครือข่ายที่เชื่อมต่ออยู่ ซึ่งอาจทำให้การวิเคราะห์แพ็คเก็ตทำได้ยากขึ้น เนื่องจากอาจมีแพ็คเก็ตที่ถูกบันทึกไว้นับหมื่นรายการ อย่างไรก็ดี ผู้ใช้งานสามารถกำหนดตัวกรอง (filter) เพื่อให้ไวร์ชาร์คดักจับเฉพาะแพ็คเก็ตที่มีหมายเลขไอพีของเครื่องเป้าหมายได้ เช่น ถ้าแฮ็กเกอร์ทราบว่ามีเครื่องใดเครื่องหนึ่งในระบบเครือข่ายขององค์กรเป็นเครื่องเซอร์ฟเวอร์ที่มีความสำคัญต่อการโจมตีก็จะกรองเอาเฉพาะแพ็คเก็ตของเครื่องนั้น ซึ่งทำให้การวิเคราะห์ข้อมูลมีความง่ายขึ้น

ตารางที่ 1 ข้อมูลของแพ็คเก็ตที่ดักจับด้วยไวร์ชาร์ค

Traffic	Captured
First-Last	584,627.56 sec
Avg. packets/sec	1.349
Avg. packets size	106 bytes
Bytes	84,033,815
Avg. bytes/sec	143.74
Avg. Mbit/sec	0.001

ตัวอย่างของข้อมูลที่เกี่ยวข้องกับเวลาของการดักจับแพ็คเก็ต ความเร็วในการดักจับ ความเร็วเฉลี่ย แบนด์วิธด์ของการส่งแพ็คเก็ต แสดงไว้ในตารางที่ 1 จะเห็นได้ว่าขนาดของแพ็คเก็ตโดยเฉลี่ยมีค่าเท่ากับ 106 bytes ซึ่งเป็นแพ็คเก็ตขนาดเล็กที่ถูกส่งอยู่บนระบบเครือข่ายข้อมูลสถิติที่ได้จากการดักจับแพ็คเก็ตโดยแบ่งตามชนิดของโปรโตคอลตามตารางที่ 2 ออกเป็น Internet, Logical-link Control, Address Resolution, IPV6, และ Internetwork Packet Exchange จำนวนแพ็คเก็ตทั้งสิ้น ประมาณ 788,000 แพ็คเก็ต ใช้เนื้อที่การจัดเก็บไฟล์ประมาณ 80 Mbytes

ตารางที่ 2 ข้อมูลสถิติที่ได้จากการดักจับแพ็คเก็ตแบ่งตามชนิดของโปรโตคอล

Protocol	%Packet	Packet	Bytes
Internet Protocol	55.02	434,013	58,931,251
Logical-Link Ctrl	39.34	310,300	22,414,698
Addr.Resolultion	5.51	43,470	2,607,552
IPV6	0.11	893	69,394
Internetwork Packet Exchange	0.02	180	10,800

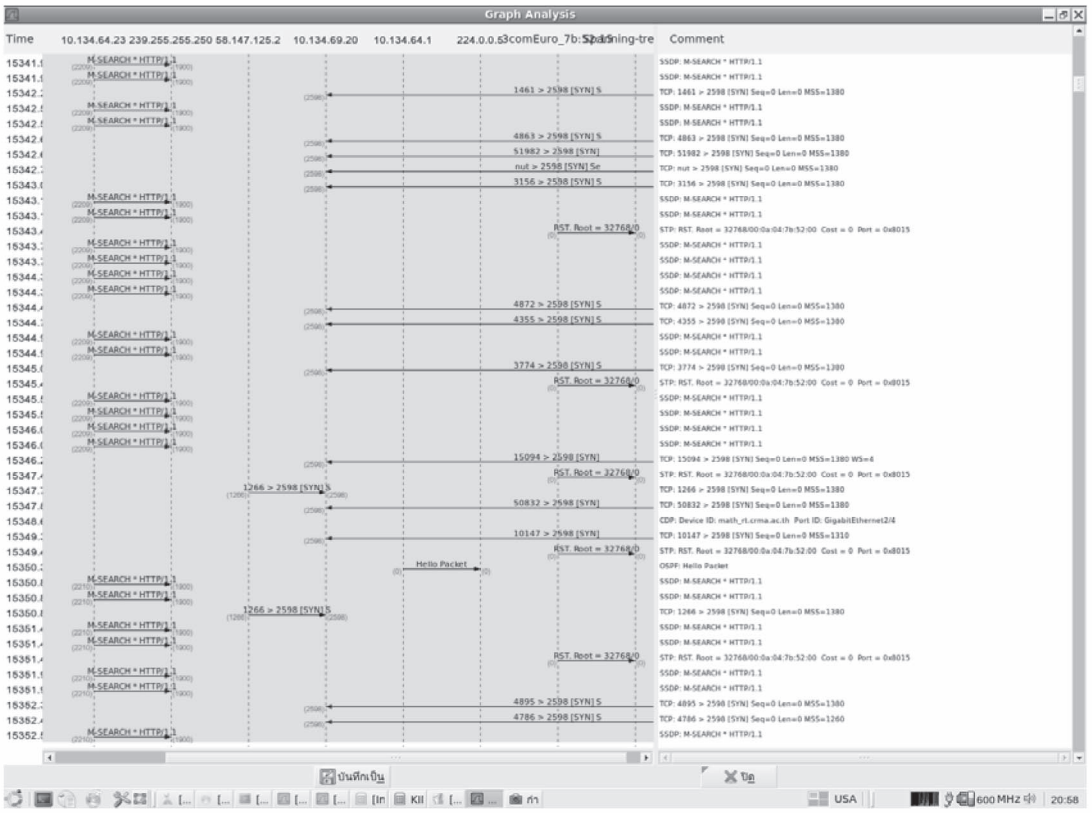
4.1 การทดลองดักจับแพ็คเก็ตของรหัสผ่าน

ในสงครามสารสนเทศเชิงรุกจะมีการดักจับแพ็คเก็ตของฝ่ายตรงข้ามโดยเฉพาะบนเครื่องที่เป็นเป้าหมายในการโจมตี ทั้งนี้เพื่อให้สามารถเจาะเข้าสู่ระบบได้ในที่สุด (2) ในการทดลองนี้ผู้เขียนได้สมมติว่ามีเครื่องคอมพิวเตอร์ที่เป็นเป้าหมายในการโจมตี แล้วใช้ไวร์ชาร์คในการดักจับแพ็คเก็ต ของการล็อกอินเข้าไปยังเครื่อง ทำให้สามารถดักจับแพ็คเก็ตที่เป็นรหัสผ่านในการเข้าเครื่อง ในกรณีที่ไม่มีการเข้ารหัสของแพ็คเก็ตจะสามารถมองเห็นรหัสผ่านในรูปแบบของรหัสแอสกี้ได้เลย แต่ในกรณีที่มีการเข้ารหัส เช่นในการใช้การล็อกอินแบบ SSH จะไม่สามารถมองเห็นรหัสผ่านได้ แต่สามารถนำข้อมูลในแพ็คเก็ตนั้นมาทำการถอดรหัส หรือใช้เทคนิค TCP Replay ในการเข้าถึงระบบได้เช่นกัน (4)

รูปที่ 4 แสดงการวิเคราะห์กราฟการเชื่อมโยงของการส่งแพ็คเก็ตในระบบเครือข่ายที่ทำการทดสอบ ซึ่งสามารถใช้ระบุปัญหาของระบบเครือข่าย หรือค้นหาเซอร์ฟเวอร์ที่ให้บริการแก่เครื่องลูกข่าย ด้วยโปรโตคอลต่างๆ รวมถึงลำดับการเชื่อมต่อระหว่างเครื่องที่รับส่งแพ็คเก็ตที่ถูกดักจับอยู่บนระบบเครือข่าย

4.2 การกรองแพ็คเก็ตที่ต้องการ

การตั้งค่าของตัวกรองในไวร์ชาร์ค เพื่อให้ดักจับเฉพาะแพ็คเก็ตที่ต้องการ และเพื่อดักจับรหัสผ่านของผู้ใช้งานที่ล็อกอินเข้ามายังเครื่องนั้น สามารถทำได้โดยใส่ตัวแปรที่ต้องการลงไปในช่อง Filter ของไวร์ชาร์ค เช่น ip.addr==10.134.64.18 ไวร์ชาร์คจะทำการกรองเอาเฉพาะแพ็คเก็ตที่เข้าออกสำหรับเครื่องนั้น ทำให้สามารถวิเคราะห์แพ็คเก็ตได้ง่ายขึ้น



รูปที่ 4 การวิเคราะห์การเชื่อมโยงระหว่างการส่งข้อมูลในระบบเครือข่าย

ตารางที่ 3 ตัวอย่างการใช้ตัวกรองในไวร์ชาร์ค

ตัวกรอง	ข้อความ
Ethernet address 00:08:15:00:08:15	eth.addr== 00:08:15:00:08:15
Ethernet type 0x0806 (ARP)	eth.type==0x0806
IP only	ip
IP address 192.168.0.1	ip.addr==192.168.0.1
TCP or UDP port is 80 (HTTP)	tcp.port==80 ‖ udp.port==80

ตัวอย่างการใช้ตัวกรองแสดงในตารางที่ 3 การกรองแพ็คเก็ตอาจทำได้ด้วยการตั้งค่าการกรอง ก่อนเริ่มดักจับแพ็คเก็ตหรือ ทำการดักจับแพ็คเก็ตทั้งหมดที่วิ่งผ่านมายังอุปกรณ์เครือข่ายของเครื่องที่ใช้ดักจับทั้ง บันทึกผลการดักจับลงในไฟล์ แล้วทำการกรองด้วยตัวแปรที่ต้องการ

ผลการทดลองในเอกสารฉบับนี้ได้จากการปฏิบัติตามขั้นตอนต่อไปนี้

- เชื่อมต่อเครื่องเซอร์ฟเวอร์ A เครื่องลูกข่าย B เครื่องแฮ็กเกอร์ C ให้อยู่บนเครือข่ายเดียวกัน
- เปิดเครื่องเซอร์ฟเวอร์ A และให้บริการเว็บ telnet และ SSH
- รันโปรแกรมไวร์ชาร์คบนเครื่อง C เพื่อดักจับแพ็คเก็ตเฉพาะเครื่องเซอร์ฟเวอร์

◉ ทดลองล็อกอินจากเครื่อง B ไปที่เว็บที่มีการถามรหัสผ่าน

◉ ทดลอง telnet หรือ ftp จากเครื่องลูกข่าย B ไปยังเครื่องแม่ข่าย A

◉ ทดลอง ssh ไปยังเครื่องแม่ข่าย A เพื่อทดสอบการเข้ารหัสของ SSH

ผลการทดลองแสดงให้เห็นว่าสามารถใช้ไวร์ชาร์คในการดักจับแพ็คเก็ต ด้วยการกรองเอาเฉพาะข้อมูลของเครื่องเป้าหมาย และสามารถแสดงรหัสผ่านการเข้าถึงเครื่องและสามารถนำไปใช้งานในปฏิบัติการสงครามสารสนเทศเชิงรุกได้

5. สรุป

ในบทความนี้ผู้เขียนได้กล่าวถึงการติดตั้งและการใช้งานไวร์ชาร์คเบื้องต้น เพื่อเป็นแนวทางในการศึกษาและนำไปใช้งานในด้านสงครามสารสนเทศเชิงรุก การแก้ปัญหาการใช้งานในระบบปฏิบัติการลินุกซ์ Ubuntu ซึ่งมีปัญหากับการเรียกใช้งานไลบรารี่ libdatrie ศึกษาการทำงานด้วยการวิเคราะห์ผลการดักจับแพ็คเก็ต การกรองแพ็คเก็ตที่ต้องการ ผลการทดสอบโปรแกรมไวร์ชาร์คแสดงให้เห็นถึงศักยภาพในการนำไปประยุกต์ใช้ในสงครามสารสนเทศเชิงรุกเพื่อใช้ในการวิเคราะห์ข้อมูลสำหรับการโจมตีเป้าหมายที่ต้องการ

กิตติกรรมประกาศ

งานวิจัยนี้ได้รับการสนับสนุนจากศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) และเป็นส่วนหนึ่งของ "โครงการความร่วมมือทางวิชาการระหว่าง สวทช. และ รร.จปร." โครงการจัดตั้งห้องปฏิบัติการเพื่อการวิจัยด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ รร.จปร. รหัสโครงการ NT-B-22-I5-99-48-11

เอกสารอ้างอิง

(1) พันเอกปรัชญา เฉลิมวัฒน์ "การใช้งาน Wireshark ในการดักจับแพ็คเก็ต", รายงานด้านเทคนิค ในผลการดำเนินการวิจัยโครงการ จัดตั้งห้องปฏิบัติการเพื่อการวิจัยด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ รร.จปร., 1 ส.ค. 50.

(2) Edward Waltz, Information Warfare: Principles and Operations, Artech House, 1998.

(3) Angela Orebaugh, Gilbert Ramirez, and Jay Beale, Wireshark & Ethereal Network Protocol Analyzer Toolkit, Syngress, 2006.

(4) Anonymous, Certified Ethical Hacker -CEH Certification boot camp on DVD, URL: http://www.cissp.com/store/product.asp?pID=64&c=83032.