บทที่ 4
ผลการวิเคราะห์ข้อมูล

องค์ความรู้ทางด้านความมั่นคงและปลอดภัยจากกรณีศึกษา

การแจ้งเตือนภัยของระบบการตรวจจับการบุกรุก

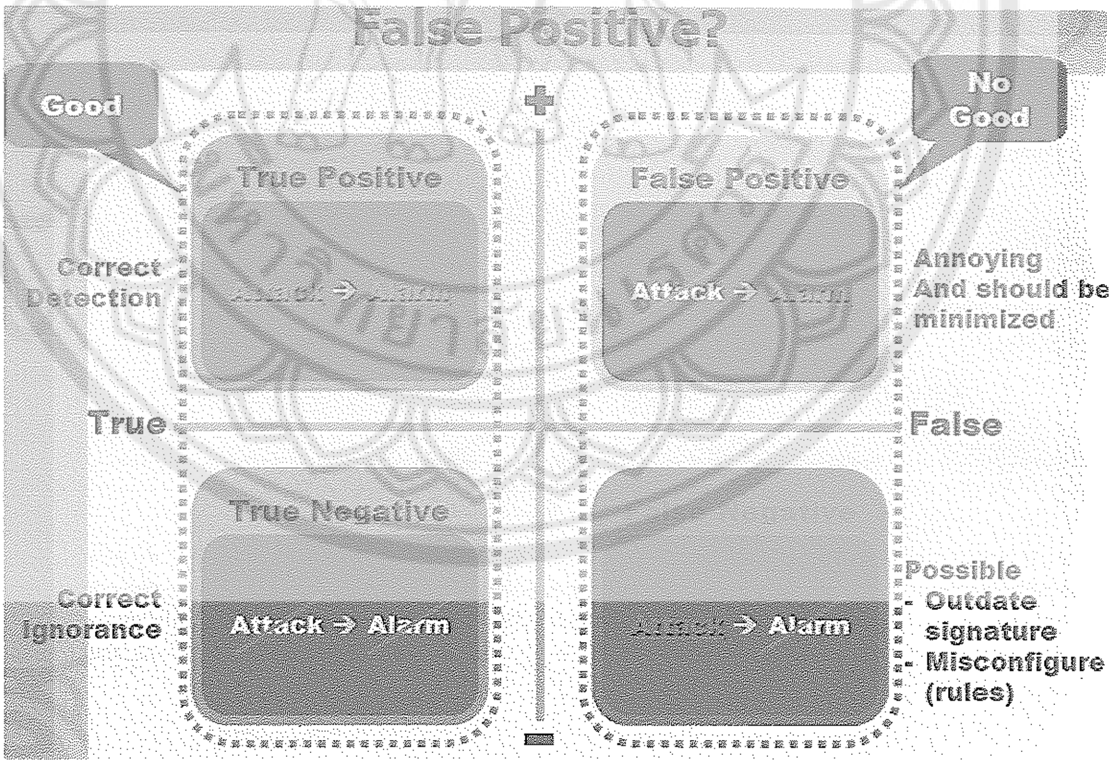
- แบ่งออกได้ดังต่อไปนี้

  การแจ้งเตือนภัยที่ไม่ดี

  - False Positive **ยังไม่มีการบุกรุกแต่กลับแจ้งเตือนภัย**
  - False Negative **มีการบุกรุกแต่กลับไม่แจ้งเตือนภัย**

  การแจ้งเตือนภัยที่ดี

  - True Positive **เมื่อมีการถูกบุกรุกต้องสามารถแจ้งเตือนภัยได้**
  - True Negative **เมื่อไม่มีการบุกรุกต้องไม่แจ้งเตือนภัย**



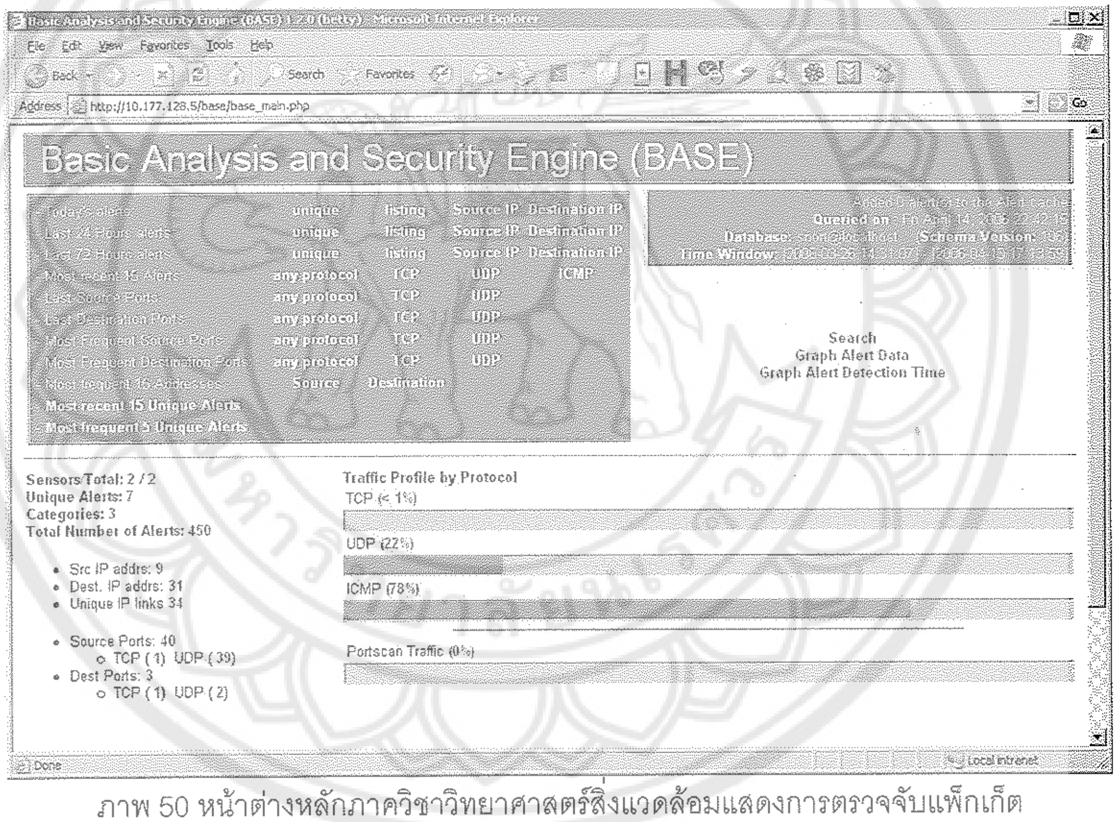
ภาพ 49 ภาพแสดงระบบการเตือนภัยที่ดีและไม่ดีของระบบการตรวจจับผู้บุกรุก

องค์ความรู้ทางด้านความมั่นคงและปลอดภัยแยกออกเป็นแต่ละภาควิชาจากการศึกษา

1. ภาควิชาวิทยาศาสตร์สิ่งแวดล้อม

การแบ่งค่าของการตรวจจับออกได้ดังต่อไปนี้

- โปโตคอล TCP มีการแจ้งเตือนภัย 1 %
- โปโตคอล UDP มีการแจ้งเตือนภัย 22 %
- โปโตคอล ICMP มีการแจ้งเตือนภัย 78 %
- Portscan Traffic มีการแจ้งเตือนภัย 0 %



ภาพ 50 หน้าต่างหลักภาควิชาวิทยาศาสตร์สิ่งแวดล้อมแสดงการตรวจจับแพ็กเก็ต

1.1 โปโตคอล TCP

มีการแจ้งเตือนภัยจำนวน 1 ครั้งดังรูป

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#0-(2-83)	[local] [snort] ATTACK-RESPONSES 403 Forbidden	2006-03-27 21:59:11	10.177.128.5:80	10.177.112.106:2220	TCP

ภาพ 51 แสดงการการแจ้งเตือนภัยโปโตคอลTCP ของภาควิชาวิทยาศาสตร์สิ่งแวดล้อม

เหตุการณ์ “ATTACK-RESPONSES 403 Forbidden”

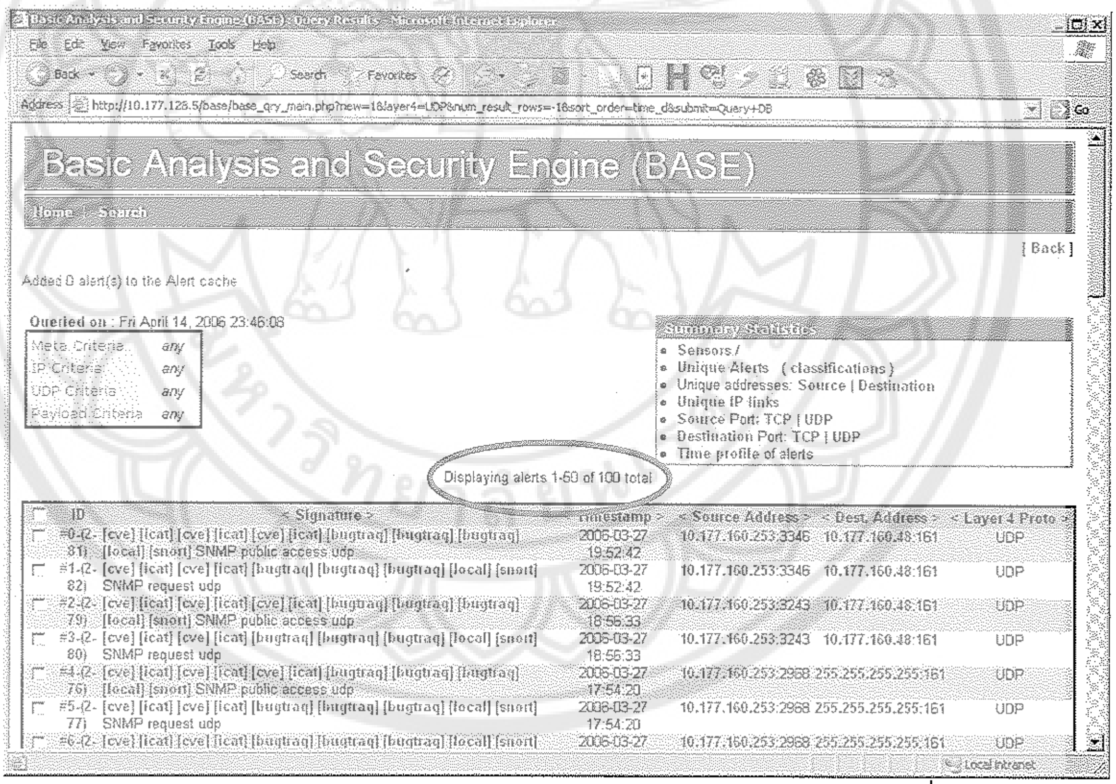
คำอธิบาย

*[1]Error 403 นั้นเป็นความผิดพลาดจากการที่ผู้ใช้พยายามเข้าใช้งานส่วนใดๆ ของเว็บไซต์โดยไม่ได้รับอนุญาต” เป็นการแจ้งเตือนภัยที่มีการพยายามเข้ามาทางรู้รั่วของบริการเว็บเซิร์ฟเวอร์ที่ใช้งาน Apache จากหมายเลขไอพี 10.177.112.106 มาที่เว็บเซิร์ฟเวอร์หมายเลขไอพี 10.177.128.5

ถือเป็นการแจ้งเตือนภัยที่เป็นแบบ True Positive

1.2 โปโตคอล UDP

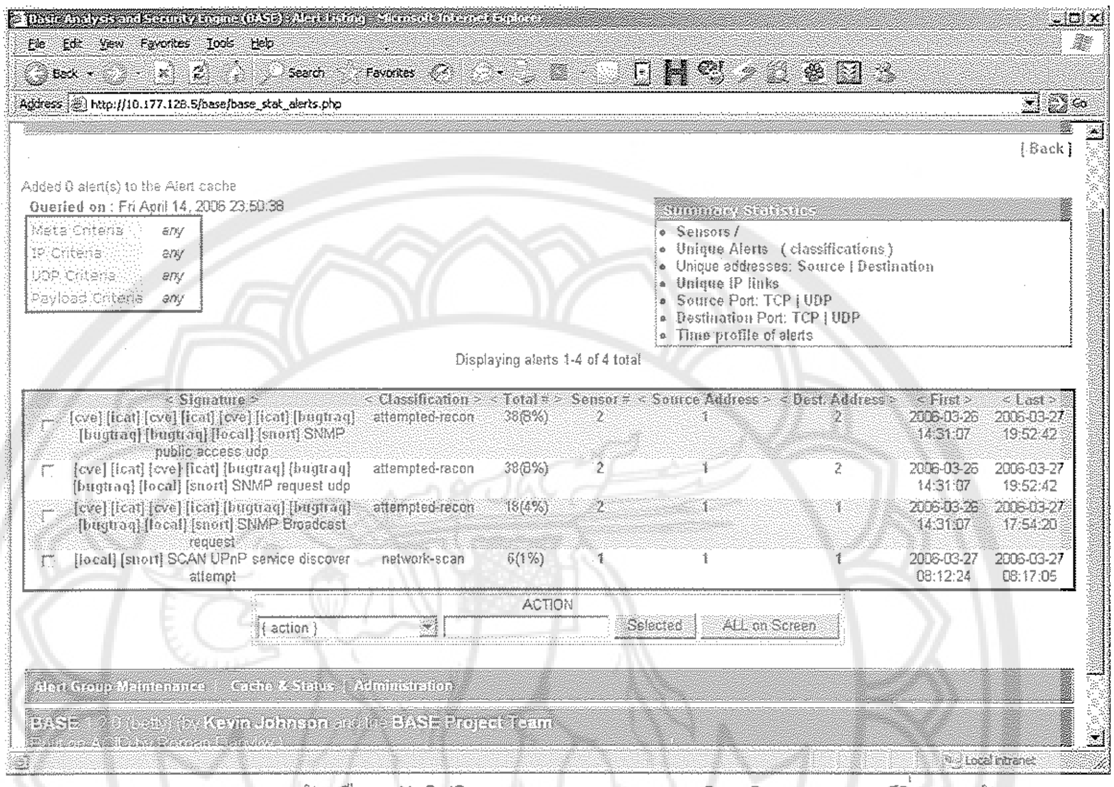
มีการแจ้งเตือนภัยจำนวน 100 ครั้งดังรูป



ภาพ 52 แสดงการการแจ้งเตือนภัยโปโตคอลUDPของภาควิชาวิทยาศาสตร์สิ่งแวดล้อม

1 มนัชยา ชมธวัช, Apache Security Checklist, http://thaicert.nectec.or.th/paper/unix_linux/apache_chklist.php#8

แยกตามหมายเลขไอพีที่มีการแจ้งเตือนภัยออกได้ดังรูป



ภาพ 53 แสดงการการแจ้งเตือนภัยโปโตคอล UDP ของภาควิชาวิทยาศาสตร์สิ่งแวดล้อม แยกตามหมายเลขไอพี

รายละเอียดของการแจ้งเตือนภัยของ UDP สามารถแบ่งออกได้ 4 เหตุการณ์ดังต่อไปนี้

1.2.1 เหตุการณ์ที่ 1 เป็นการแจ้งเตือนภัยที่มีข้อความแจ้งว่า “SNMP public access udp” ทั้งหมด 38 ครั้ง

1.2.2 เหตุการณ์ที่ 2 เป็นการแจ้งเตือนภัยที่มีข้อความแจ้งว่า “SNMP request udp” ทั้งหมด 38 ครั้ง

1.2.3 เหตุการณ์ที่ 3 เป็นการแจ้งเตือนภัยที่มีข้อความแจ้งว่า “SNMP Broadcast request” ทั้งหมด 18 ครั้ง

คำอธิบาย เป็นช่วงโหว่ SNMP Service

ถือเป็นการแจ้งเตือนภัยที่เป็นแบบ True Positives

[2]คำอธิบาย

Simple Network Managament Protocol (SNMP) ถูกนำมาใช้งานอย่างแพร่หลายในปัจจุบัน เพื่อการเฝ้าตรวจและปรับแต่งค่าอุปกรณ์เกือบทุกชนิดที่สามารถทำงานผ่านโพรโตคอล TCP/IP ได้ โพรโตคอล SNMP ถูกนำไปใช้งานอย่างกว้างขวางและมีการทำงานข้ามแพลตฟอร์มต่างๆ ของเครือข่าย ประโยชน์หลักของโพรโตคอล SNMP คือสามารถใช้เป็นวิธีการหนึ่งในการปรับแต่งการทำงานและจัดการอุปกรณ์ เช่น เครื่องพิมพ์ (พรินเตอร์) เราเตอร์ สวิตช์ เป็นต้น หรือใช้ในการส่งค่าอินพุตไปยังบริการที่ทำหน้าที่เฝ้าตรวจเครือข่าย

การติดต่อแบบ Simple Network Management ประกอบด้วยการแลกเปลี่ยนข้อความที่มีรูปแบบต่างๆ ระหว่างเครื่องที่ทำหน้าที่บริหาร SNMP (SNMP management station) กับอุปกรณ์เครือข่ายซึ่งมีการเปิดใช้งานซอฟต์แวร์ชนิดที่นิยมเรียกว่าซอฟต์แวร์เอเจนต์ (agent software) วิธีการทำงานของโพรโตคอล SNMP ดังกล่าวนี้ทำให้เกิดช่องโหว่ซึ่งผู้บุกรุกสามารถนำไปใช้โจมตีได้ทั้งจากวิธีการจัดการข้อความที่ถูกส่ง และจากกลไกการพิสูจน์ตัวตนผู้ใช้งานในระหว่างการจัดการข้อความ

ช่องโหว่ที่เกิดจากวิธีการซึ่งโพรโตคอล SNMP เวอร์ชัน 1 จัดการและรอรับข้อความได้แสดงรายละเอียดไว้ใน CERT Advisory CA-2002-03 ช่องโหว่ที่ปรากฏจำนวนหนึ่งเกิดจากวิธีการจัดการและการถอดรหัสในขั้นตอนของการร้องขอข้อมูลและการรอรับข้อความทั้งจากฝั่งเครื่องคอมพิวเตอร์ที่ทำหน้าที่บริหาร SNMP และฝั่งซอฟต์แวร์เอเจนต์ ช่องโหว่เหล่านี้มิได้เกิดขึ้นเมื่อนำโพรโตคอล SMNP ไปใช้งานรูปแบบใดรูปแบบหนึ่งโดยเฉพาะ แต่ส่งผลกับผลิตภัณฑ์ที่ใช้งานโพรโตคอล SNMP จากหลายผู้ผลิต ผลจากการโจมตีผ่านทางช่องโหว่นี้มีความแตกต่างกันออกไปตั้งแต่การทำให้ระบบไม่สามารถให้บริการได้จากผลของการ denial of service ไปจนถึงการทำให้การจัดการและการทำงานของอุปกรณ์ที่เปิดใช้งานโพรโตคอล SNMP ผิดไปจากที่ต้องการ

กลไกการพิสูจน์ตัวตนผู้ใช้ที่มีใช้งานในโพรโตคอล SNMP เวอร์ชันเก่ายังคงถูกรวมไว้ในการทำงานของโพรโตคอล SNMP เวอร์ชันต่อๆ มา ทำให้ถูกใช้เป็นช่องโหว่สำคัญของระบบ กลไกการพิสูจน์ตัวตนผู้ใช้ที่มีในโพรโตคอล SNMP เวอร์ชัน 1 และเวอร์ชัน 2 คือการใช้ "community string" ที่ไม่มีการเข้ารหัสเท่านั้น การขาดการเข้ารหัสทำให้ระบบเกิดความเสี่ยงที่ผู้บุกรุกจะนำไปใช้ในการโจมตี

---

2 ศิริวรรณ อภิสิริเดช และ มนัชยา ชมธวัชม, **20 ช่องโหว่สำคัญที่เป็นอันตรายร้ายแรงต่อความปลอดภัยของอินเทอร์เน็ต 20 ช่องโหว่สำคัญที่เป็นอันตรายร้ายแรงต่อความปลอดภัยของอินเทอร์เน็ต**, http://www.thaicert.nectec.or.th/paper/basic/top20.php

ได้ อย่างไรก็ตาม ช่องโหว่ของโพรโตคอล SNMP มิได้มีเพียงที่อธิบายไปแล้วเท่านั้น เนื่องจากค่าดีฟอลต์ของ community string ที่ถูกกำหนดให้กับอุปกรณ์ที่ใช้งาน SNMP เกือบทั้งหมดคือ "public" และผู้ผลิตอุปกรณ์เครือข่ายบางรายได้พยายามแก้ไขค่า community string ที่ใช้เป็น "private" สำหรับการส่งผ่านข้อมูลที่มีความอ่อนไหวกว่า ผู้บุกรุกสามารถใช้ช่องโหว่ของโพรโตคอล SNMP ที่กล่าวมานี้ เพื่อแก้ไขหรือหยุดการทำงานของอุปกรณ์ต่างๆ ได้จากเครือข่ายภายนอก นอกจากนั้น การรอรับข้อความที่ถูกส่งด้วยโพรโตคอล SNMP จะทำให้ผู้บุกรุกทราบถึงผังโครงสร้างของเครือข่ายที่ใช้งาน รวมถึงระบบและอุปกรณ์ที่เชื่อมต่อกับเครือข่ายนั้น ผู้บุกรุกจะใช้ข้อมูลเหล่านี้เพื่อเลือกเป้าหมายและวางแผนการโจมตี

ผู้ผลิตและผู้จำหน่ายส่วนใหญ่นิยมกำหนดให้โพรโตคอล SNMP เวอร์ชัน 1 ทำงานโดยดีฟอลต์ และหลายรายไม่ได้รวมเอาความสามารถในการใช้งานโพรโตคอล SNMP เวอร์ชัน 3 ซึ่งมีความปลอดภัยและสามารถปรับแต่งแก้ไขเพื่อปรับปรุงวิธีการพิสูจน์ตัวตนผู้ใช้รวมไว้ในอุปกรณ์ของตน อย่างไรก็ตาม ผู้ใช้งานสามารถนำออปชันนี้มาใช้งานกับอุปกรณ์ของตนเพื่อรองรับการทำงานของโพรโตคอล SNMP เวอร์ชัน 3 ได้โดยไม่เสียค่าใช้จ่ายใดๆ ภายใต้ลิขสิทธิ์ของ GPL หรือ BSD

โพรโตคอล SNMP ไม่ได้มีใช้งานบนระบบปฏิบัติการ Unix เท่านั้น มีการนำโพรโตคอล SNMP ไปใช้งานอย่างกว้างขวางในระบบปฏิบัติการ Windows ในอุปกรณ์เครือข่าย เครื่องพิมพ์ และอุปกรณ์ชนิดฝังตัว แต่การโจมตีที่เกี่ยวข้องกับการทำงานของโพรโตคอล SNMP ส่วนใหญ่ที่พบเกิดขึ้นกับระบบปฏิบัติการ Unix ที่ค่า configuration ซึ่งกำหนดการทำงานของโพรโตคอล SNMP ที่เปิดใช้งานขาดความปลอดภัย

U4.2 ระบบปฏิบัติการที่ได้รับผลกระทบ ระบบปฏิบัติการ Unix และ Linux เกือบทั้งหมดที่มีการติดตั้งให้ใช้งานโพรโตคอล SNMP และโดยส่วนใหญ่จะถูกเปิดใช้งานโดยดีฟอลต์ นอกจากนั้น อุปกรณ์เครือข่ายและระบบปฏิบัติการอื่นๆ ที่เปิดใช้งานโพรโตคอล SNMP หลายๆ ระบบก็ได้รับผลกระทบจากช่องโหว่นี้เช่นกัน

วิธีการป้องกันอันตรายจากช่องโหว่นี้

- **ช่องโหว่ที่เกิดจากการจัดการการร้องขอและการรอรับ**:
    1. หากไม่มีความต้องการใช้งานโพรโตคอล SNMP ให้ยกเลิกการทำงานที่อุปกรณ์หรือระบบนั้นๆ

2. เมื่อเป็นไปได้ ให้นำเอาโพรโตคอล SNMP เวอร์ชัน 3 (SNMPv3) ซึ่งมีรูปแบบการทำงานที่เน้นความปลอดภัยของผู้ใช้มาใช้ร่วมกับการตรวจสอบพิสูจน์ข้อความที่ส่ง และอาจใช้การเข้ารหัสข้อมูลแต่ละหน่วยของโพรโตคอล
3. หากจำเป็นต้องใช้งานโพรโตคอล SNMP เวอร์ชัน 1 หรือเวอร์ชัน 2 จะต้องตรวจสอบให้แน่ใจว่า ได้ใช้งานเวอร์ชันที่ได้รับการอัพเดต patch ล่าสุดจากผู้ผลิตเท่านั้น สำหรับการขอรับทราบข้อมูลเฉพาะจากผู้ผลิตและผู้จำหน่ายแต่ละรายสามารถค้นหาได้จากหัวข้อ "Appendix A" ของ CERT Advisory CA-2002-03
4. กรองข้อมูลที่ส่งผ่านโพรโตคอล SNMP (พอร์ต 161 TCP/UDP และพอร์ต 162 TCP/UDP) ที่ทางเข้าของเครือข่าย หากไม่มีความจำเป็นต้องเรียกใช้หรือจัดการใดๆ จากภายนอก
5. ใช้การควบคุมการเข้าถึงโดยกำหนดเครื่องที่จะสามารถเรียกใช้ระบบของเอเจนต์ SNMP ที่ใช้งาน หากเกิดปัญหาจากข้อจำกัดเรื่องความสามารถของเอเจนต์ในระบบปฏิบัติการ อาจใช้การควบคุมว่าจะอนุญาตให้เอเจนต์ที่ใช้งานตอบรับการร้องขอจากเครื่องใดบ้างแทนได้ สำหรับระบบปฏิบัติการ Unix โดยทั่วไปสามารถทำได้โดยการแก้ไขค่า configuration ของ TCP-Wrappers หรือ Xinetd และอาจใช้ไฟร์วอลล์บนเครื่องคอมพิวเตอร์ใดๆ กรองแพ็กเก็ตและปิดกั้นการร้องขอ SNMP ที่เข้ามา

- **ช่องโหว่ที่เกิดจาก string ใด ๆ ที่เกี่ยวข้องกับการทำงาน เป็นค่าที่ถูกกำหนดโดยยดีฟอลต์หรืออาจถูกคาดเดาได้ง่าย:**
  1. หากไม่มีความต้องการใช้งานโพรโตคอล SNMP ให้ยกเลิกการทำงานที่อุปกรณ์หรือระบบนั้นๆ
  2. เมื่อเป็นไปได้ ให้นำเอาโพรโตคอล SNMP เวอร์ชัน 3 (SNMPv3) ซึ่งมีรูปแบบการทำงานที่เน้นความปลอดภัยของผู้ใช้มาใช้ร่วมกับการตรวจสอบพิสูจน์ข้อความที่ส่ง และอาจใช้การเข้ารหัสข้อมูลแต่ละหน่วยของโพรโตคอล
  3. หากจำเป็นต้องใช้งานโพรโตคอล SNMP เวอร์ชัน 1 หรือเวอร์ชัน 2 ให้กำหนดชื่อ community string ที่ปลอดภัยโดยให้เป็นไปตามนโยบายการตั้งและการใช้งานรหัสผ่าน ตรวจสอบให้แน่ใจว่า community string และรหัสผ่านที่ใช้งานยากต่อการค้นหาหรือการคาดเดา รวมถึงได้รับการเปลี่ยนแปลงทุกระยะ
  4. ทดสอบและตรวจสอบชื่อของ community โดยใช้เครื่องมือ snmpwalk โดยสามารถค้นหาข้อมูลเพิ่มเติมได้จาก

http://www.zend.com/manual/function.snmpwalk.php และศึกษาคำแนะนำเพิ่มเติมเกี่ยวกับเครื่องมือนี้ได้ที่

http://www.sans.org/newlook/resources/IDFAQ/SNMP.htm

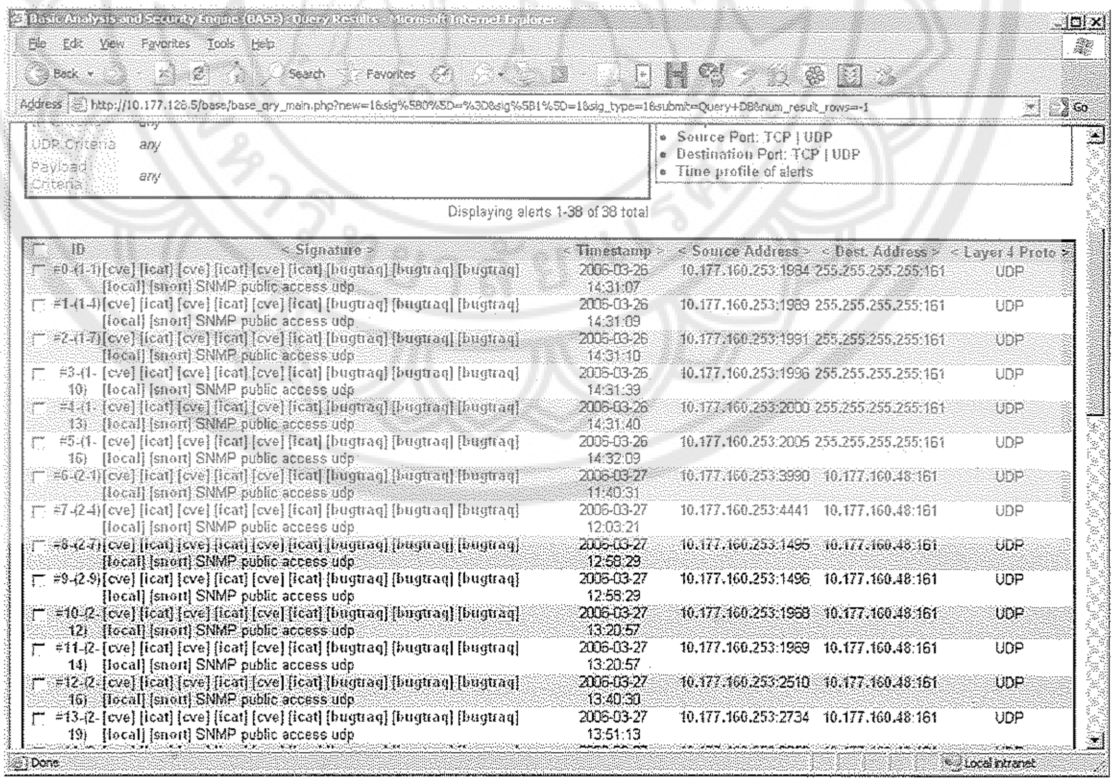
5. กรองข้อมูลที่ส่งผ่านโพรโตคอล SNMP (พอร์ต 161 TCP/UDP และพอร์ต 162 TCP/UDP) ที่ทางเข้าของเครือข่าย หากไม่มีความจำเป็นต้องเรียกใช้หรือจัดการใดๆ จากภายนอก

ในบางอุปกรณ์ หากเป็นไปได้ให้กำหนด MIBs เป็นแบบอ่านอย่างเดียว (read-only) โดยสามารถศึกษาข้อมูลเพิ่มเติมได้จาก

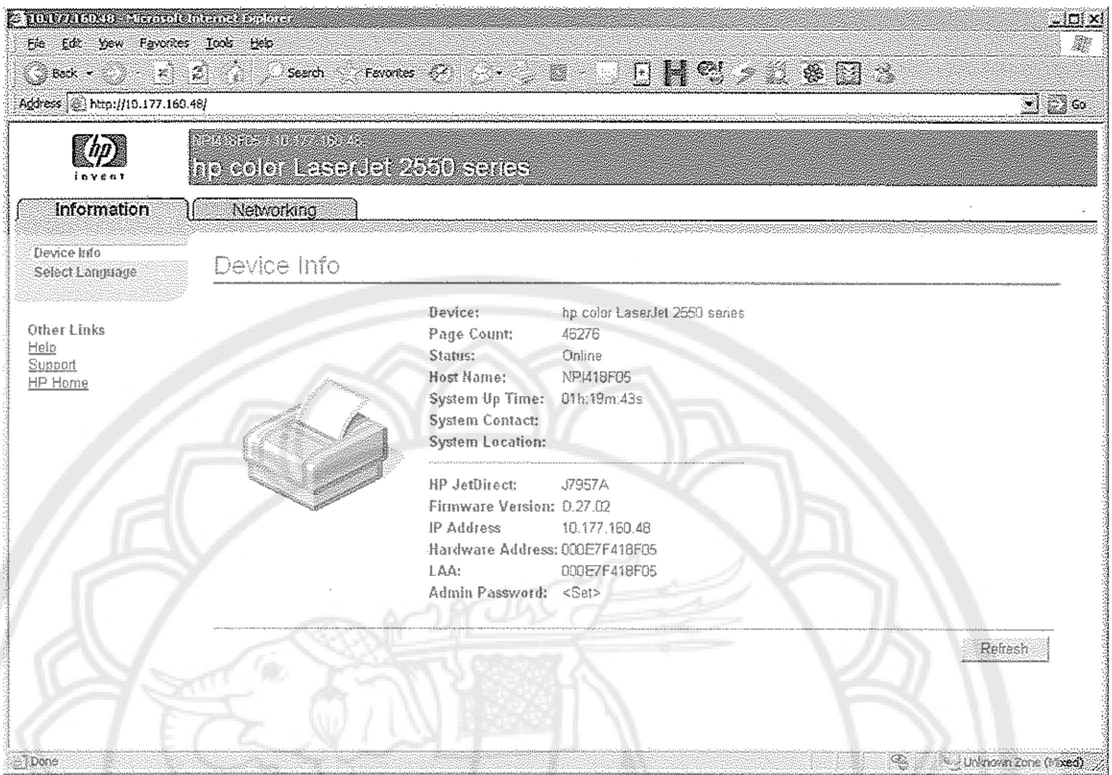
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm#ocid210315

หมายเหตุ

จากการแจ้งเตือนภัยของภาควิชาวิทยาศาสตร์สิ่งแวดล้อมนั้นก็ยังมีเหตุการณ์ที่แจ้งเตือนภัยที่แท้จริงระหว่างอุปกรณ์ที่เป็นเหตุการณ์ที่ใช้ร้องขอติดต่อผ่านโปโตคอล SNMP ด้วย port 161 ระหว่างระหว่าง File Server = 10.177.160.253 กับ Printer Server = 10.177.160.48 เพื่อใช้ตรวจสอบสถานการณ์พิมพ์งานของเครื่อง HP รุ่น laserjet 2550tn



ภาพ 54 แสดงการแจ้งเตือนภัยโปโตคอลUDP “SNMP public access udp”



ภาพ 55 แสดงหมายเลขไอพี 10.177.160.48 ว่าเป็นเครื่องให้บริการงานพิมพ์

1.2.4 เหตุการณ์ที่ 4 เป็นการแจ้งเตือนภัยที่มีข้อความแจ้งว่า “SCAN UPnP service discover attempt” ทั้งหมด 6 ครั้ง

- [3]The Universal Plug and Play (UPnP) เป็นบริการที่อนุญาตให้เครื่องคอมพิวเตอร์สามารถค้นหาและใช้งานอุปกรณ์อื่น เช่น เครื่องคอมพิวเตอร์ สแกนเนอร์ เครื่องพิมพ์ ผ่านทางเครือข่ายได้ โดยปกติแล้ว Windows 98, 98SE ไม่มีคุณสมบัติของ UPnP ภายในตัวเอง แต่อาจจะถูกติดตั้งเพิ่มเติมผ่านทาง Internet Connection Sharing client ซึ่งติดมากับ Windows XP ได้

UPnP มีช่องโหว่ที่ถูกค้นพบในขณะนี้ 2 จุดด้วยกัน ช่องโหว่แรกเกี่ยวข้องกับ buffer overrun ซึ่งหากผู้บุกรุกส่ง NOTIFY directive ที่ผิดปกติมายังเครื่องเป้าหมายแล้ว จะทำให้ผู้บุกรุกสามารถควบคุมเครื่องเป้าหมายได้ทันที ส่วนช่องโหว่ที่สองนั้นเกิดขึ้นเนื่องจาก UPnP ไม่สามารถจำกัดขั้นตอนของการค้นหาข้อมูลจากอุปกรณ์ใหม่ที่ถูกค้นพบ โดยปกติแล้วอุปกรณ์ใหม่จะส่ง NOTIFY directive มาเพื่อแจ้งว่าให้เครื่องที่รัน UPnP สามารถค้นหาข้อมูลเพิ่มเติมเกี่ยวกับบริการของ

[3] ภูวดล ด่านระหาญ, Microsoft Security Bulletin MS01-059, http://thaicert.nectec.or.th/bulletin/microsoft/ms01-059.php

อุปกรณ์ใหม่ และวิธีในการเข้าใช้งานได้จากที่ใด ซึ่งอุปกรณ์ที่ทำหน้าที่อธิบายดังกล่าวอาจจะเป็น third-party server ซึ่งไม่ใช่อุปกรณ์ใหม่ดังกล่าวก็ได้ และ UPnP เองไม่สามารถทำงานตามกระบวนการดังกล่าวได้ ก่อให้เกิดการโจมตีแบบ DoS (Denial of Service) ที่แตกต่างกัน 2 รูปแบบด้วยกันคือ

- รูปแบบแรก ผู้บุกรุกจะส่ง NOTIFY directive มายังเครื่องที่รัน UPnP เพื่อแจ้งว่าให้ไปดาวน์โหลดข้อมูลที่อธิบายการใช้งานอุปกรณ์ตัวใหม่ได้จากเซิร์ฟเวอร์ใด และ port ใด ถ้าเซิร์ฟเวอร์ถูกตั้งให้รัน echo service ใน port ดังกล่าว แล้ว เครื่องคอมพิวเตอร์ที่รัน UPnP ดังกล่าวจะเกิดการวนลูปของการดาวน์โหลดที่ว่างเปล่า ทำให้ทรัพยากรภายในเครื่องถูกใช้ไปจนหมด ผู้บุกรุกสามารถส่ง message ดังกล่าวนี้ไปยังเป้าหมายได้โดยตรงโดยใช้หมายเลขไอพีแอดเดร็ส หรืออาจจะส่ง message ดังกล่าวไปยัง broadcast address เพื่อส่งให้กับทุกเครื่องที่อยู่ในเครือข่ายเดียวกัน ซึ่งก่อให้เกิดการโจมตีที่รุนแรงมากขึ้น
- รูปแบบที่สอง ผู้บุกรุกจะส่งรายชื่อเซิร์ฟเวอร์ที่เป็น third-party มาให้ผ่านทาง NOTIFY directive ซึ่งหากมีเครื่องเซิร์ฟเวอร์ใดสนองตอบ (response) ก็จะก่อให้เกิดการโจมตีแบบ flood ไปยัง third-party server ดังกล่าวได้ ถือได้ว่าเป็นการโจมตีแบบ DDoS (Distributed Denial of Service) ซึ่งเช่นเดียวกันกับแบบแรก ผู้บุกรุกสามารถส่ง message ดังกล่าวนี้ไปยังเป้าหมายได้โดยตรงโดยใช้หมายเลขไอพีแอดเดร็ส หรืออาจจะส่ง message ดังกล่าวไปยัง broadcast address เพื่อส่งให้กับทุกเครื่องที่อยู่ในเครือข่ายเดียวกัน ซึ่งก่อให้เกิดการโจมตีที่รุนแรงมากขึ้น

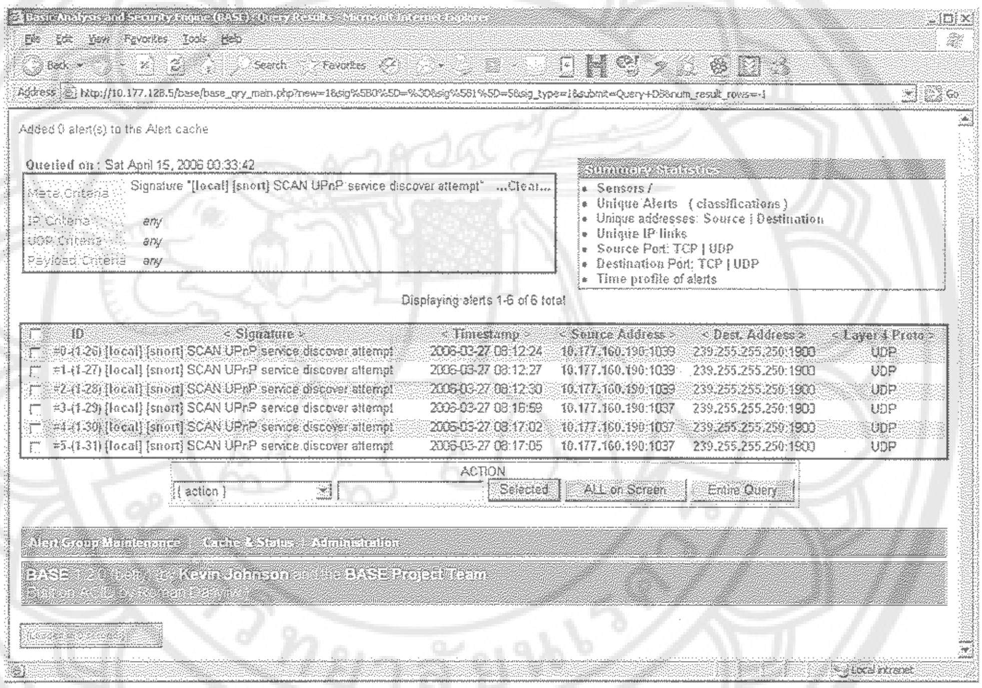
ข้อมูลเพิ่มเติม

- Windows 98 และ 98SE ซึ่งโดยปกติแล้วไม่ได้ติดตั้ง UPnP หากติดตั้ง Internet Connection Sharing client จาก WindowsXP ที่ไม่ได้ติดตั้ง patch ก็จะได้รับผลกระทบด้วย
- Windows 98 และ 98SE ที่ติดตั้ง Internet Connection Sharing client จาก WindowsXP ที่ติดตั้ง patch แล้ว จะไม่ได้รับผลกระทบจากช่องโหว่นี้ด้วย
- Windows ME จะถูกติดตั้ง UPnP มาโดย default แต่ไม่ได้ถูกรันอยู่ (ผู้ผลิต (OEM) บางรายอาจติดตั้งและรัน UPnP โดย default ซึ่งถือว่าได้รับผลกระทบจากช่องโหว่นี้)

- WindowsXP จะรัน Internet Connection Firewall โดยอัตโนมัติ ซึ่งจะทำให้ผู้บุกรุกโจมตีได้ลำบากขึ้น แต่อย่างไรก็ตามผู้บุกรุกสามารถโจมตีผ่าน broadcast, multicast หรือ unicast address ได้

การป้องกันระบบในขณะที่ยังไม่ได้ติดตั้ง patch (สำหรับ network administrator)

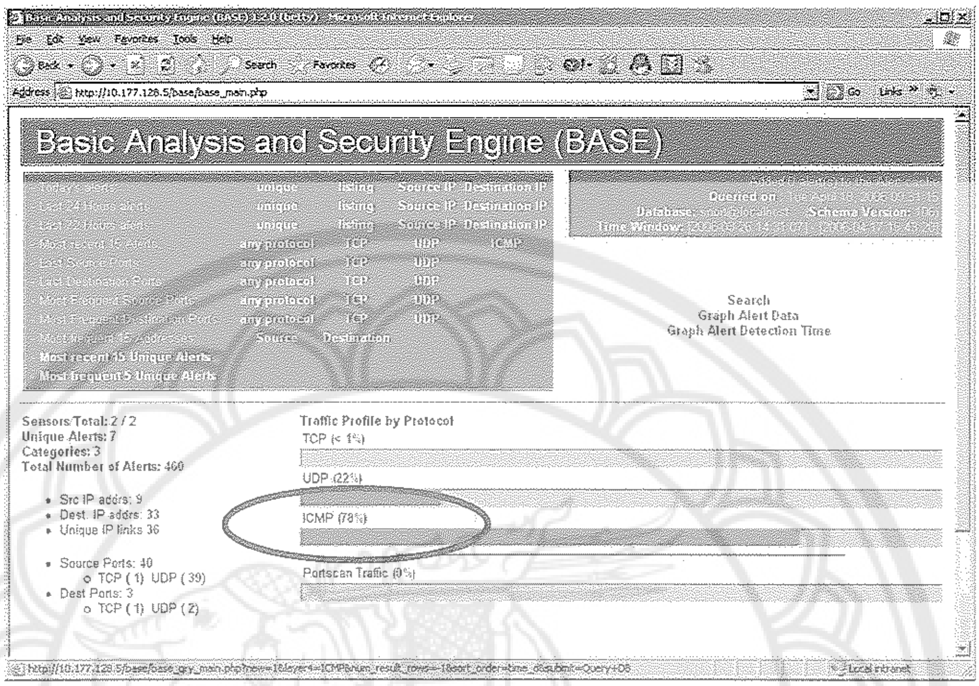
- ให้จำกัดการเข้าถึง port 1900 และ 5000 ไม่ให้มีการเรียกเข้ามาใช้จากภายนอก แต่การป้องกันด้วยวิธีนี้ไม่สามารถป้องกันการโจมตีจากภายในเครือข่ายเดียวกันได้



ภาพ 56 แสดงการแจ้งเตือนภัยโปโตคอล UDP จากหมายเลข 10.177.160.190 ส่ง message ดังกล่าวไปยัง broadcast address

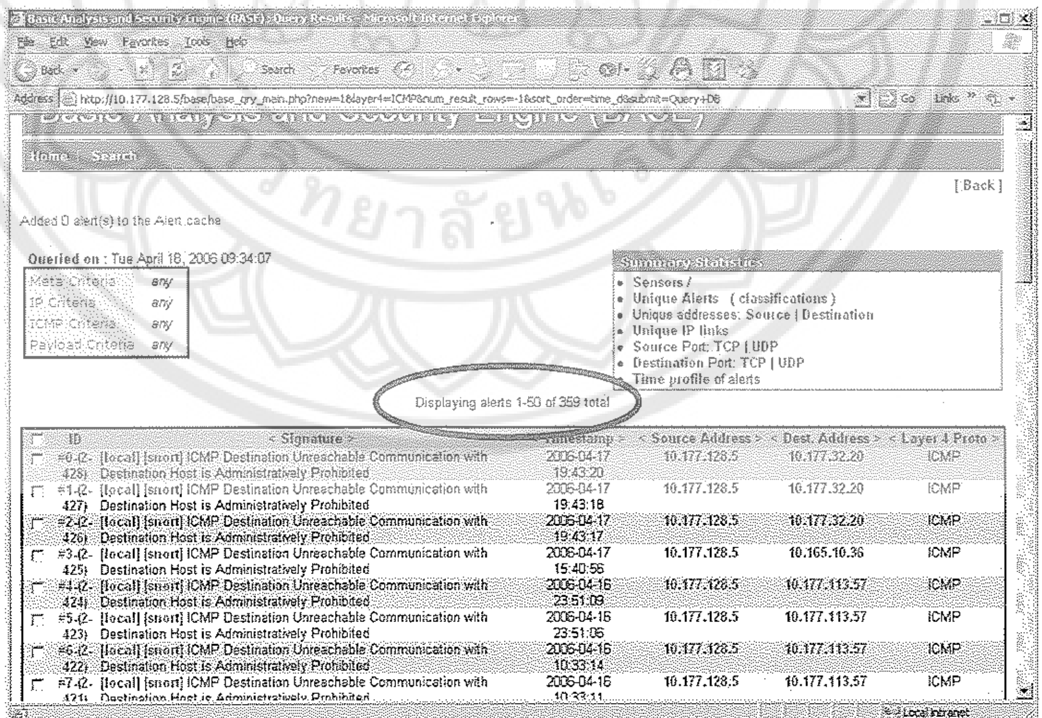
ถือเป็นการแจ้งเตือนภัยที่เป็นแบบ True Positives

1.3 โปโตคอล ICMP



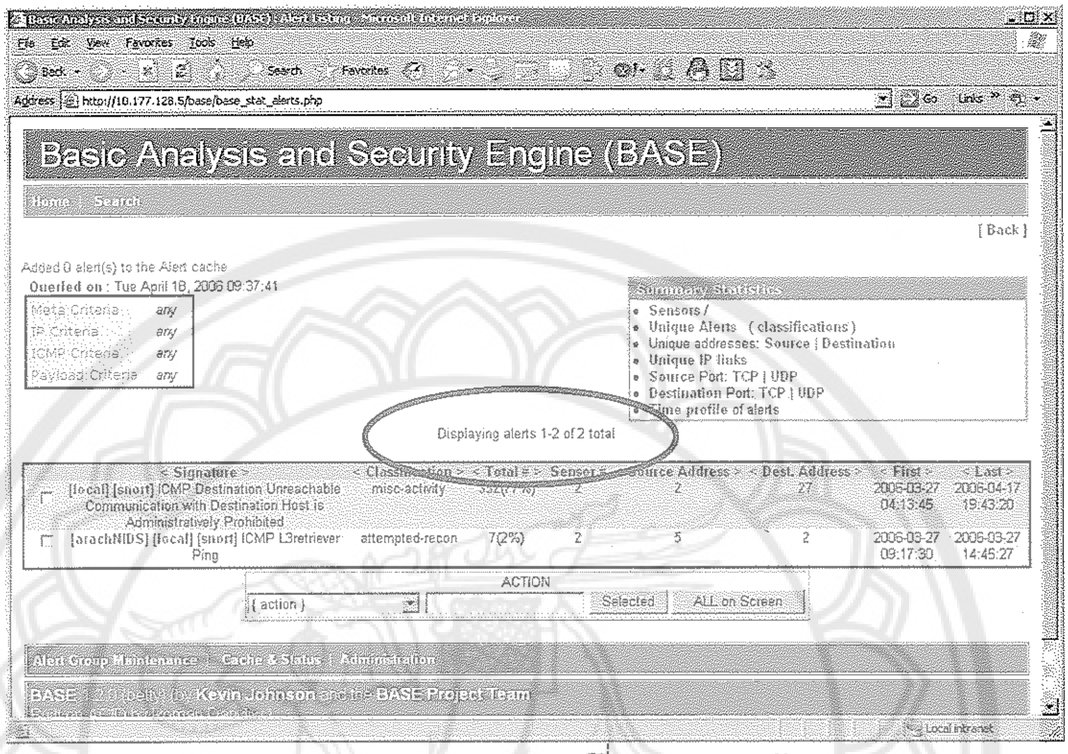
ภาพ 57 แสดงการตรวจจับการบุกรุก ICMP เป็น 78 %

มีการแจ้งเตือนภัยจำนวน 359 ครั้งดังรูป



ภาพ 58 แสดงการแจ้งเตือนภัยเป็นจำนวน 359 ครั้ง

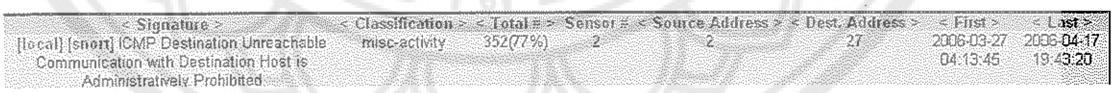
แบ่งแยกตามเหตุการณ์ที่สามารถตรวจจับการบุกรุกได้ ดังต่อไปนี้



ภาพ 59 แสดงแบ่งแยกตามเหตุการณ์ที่สามารถตรวจจับการบุกรุก

แบ่งออกได้ 2 เหตุการณ์

1.3.1 เหตุการณ์ "ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited " จำนวนทั้งสิ้น 352 ครั้ง



< Signature >	< Classification >	< Total # >	Sensor #	< Source Address >	< Dest. Address >	< First >	< Last >
[local] [snort] ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	misc-activity	352(77%)	2	2	27	2006-03-27 04:13:45	2006-04-17 19:43:20

ภาพ 60 แสดงเหตุการณ์ของการแจ้งเตือนภัยโปโตคอล ICMP "ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited "

"ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited " เป็นเหตุการณ์ที่สามารถอธิบายได้ดังข้อความข้างล่างต่อไปนี้

คำอธิบาย

ICMP ชนิดไม่สามารถติดต่อสถานีปลายทาง

เป็นการแจ้งเตือนภัยเกี่ยวกับการป้องกันการโจมตีที่เกิดขึ้นแบบ Denial of Service

ซึ่งหาก router ไม่สามารถส่ง datagram ไปยัง router หรือ host ถัดไปได้ router จะตอบกลับด้วย ICMP และใส่รหัสในฟิลด์ code เพื่อบอกสาเหตุของปัญหา

0 7	8 15	16 31
Type = 3	Code = 0 – 15	Checksum
ไม่ใช้งาน (มีค่าเป็น 0)		
Header IP + 64 bit แรกของข้อมูล		

ภาพ 61 ICMP datagram

Code	ความผิดพลาด	ความหมาย
0	Network unreachable	ไปไม่ถึงเครือข่าย
1	Host unreachable	ไปไม่ถึง host
2	Protocol unreachable	ไปไม่ถึง protocol ปลายทาง
3	Port unreachable	ไปไม่ถึง port
4	Fragmentation needed but the Do Not Fragment bit was set	จำเป็นต้องแบ่ง datagram แต่มีการกำหนดไม่ให้แบ่งแยก
5	Source route failed	เส้นทางที่กำหนดล้มเหลว
6	Destination network unknown	ไม่ปรากฏเครือข่ายปลายทาง
7	Destination host unknown	ไม่ปรากฏ host ปลายทาง
8	Source host isolated (obsolete)	
9	Destination network administratively prohibited	มีการป้องกันไม่ให้เข้าเครือข่ายปลายทาง
10	Destination host administratively prohibited	มีการป้องกันไม่ให้เข้า host ปลายทาง

ภาพ 62 Code ของ ICMP

ถือเป็นการแจ้งเตือนภัยที่เป็นแบบ True Positive

1.3.2 เหตุการณ์ที่ 2 "ICMP L3retriever Ping" จำนวนทั้งสิ้น 7 ครั้ง

< Signature >	< Classification >	< Total # >	Sensor #	< Source Address >	< Dest. Address >	< First >	< Last >
[arachNIDS] [local] [snort] ICMP L3retriever Ping	attempted-recon	7(1%)	2	5	2	2006-03-27 09:17:30	2006-03-27 14:45:27

ภาพ 63 แสดงเหตุการณ์ของการแจ้งเตือนภัยโปโตคอล ICMP "ICMP L3retriever Ping"

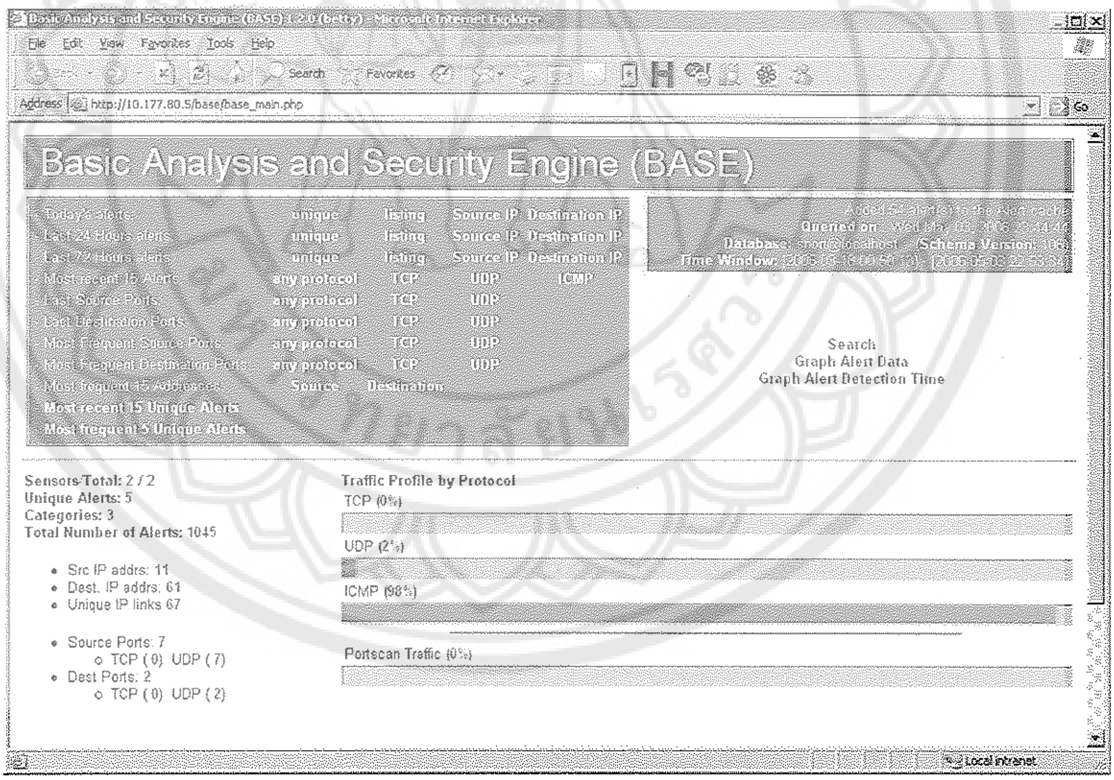
เป็นข้อความแจ้งเตือนภัยของ [4]ICMP echo request จากเครื่องที่ใช้ L3 "Retriever 1.5" ในการสแกน

ถือเป็นการแจ้งเตือนภัยที่เป็นแบบ True Positives

2. ภาควิชาชีววิทยา

การตรวจจับออกเป็นสัดส่วนได้ดังต่อไปนี้

- โปโตคอล TCP มีการแจ้งเตือนภัย 0 %
- โปโตคอล UDP มีการแจ้งเตือนภัย 2 %
- โปโตคอล ICMP มีการแจ้งเตือนภัย 98 %
- Portscan Traffic มีการแจ้งเตือนภัย 0 %

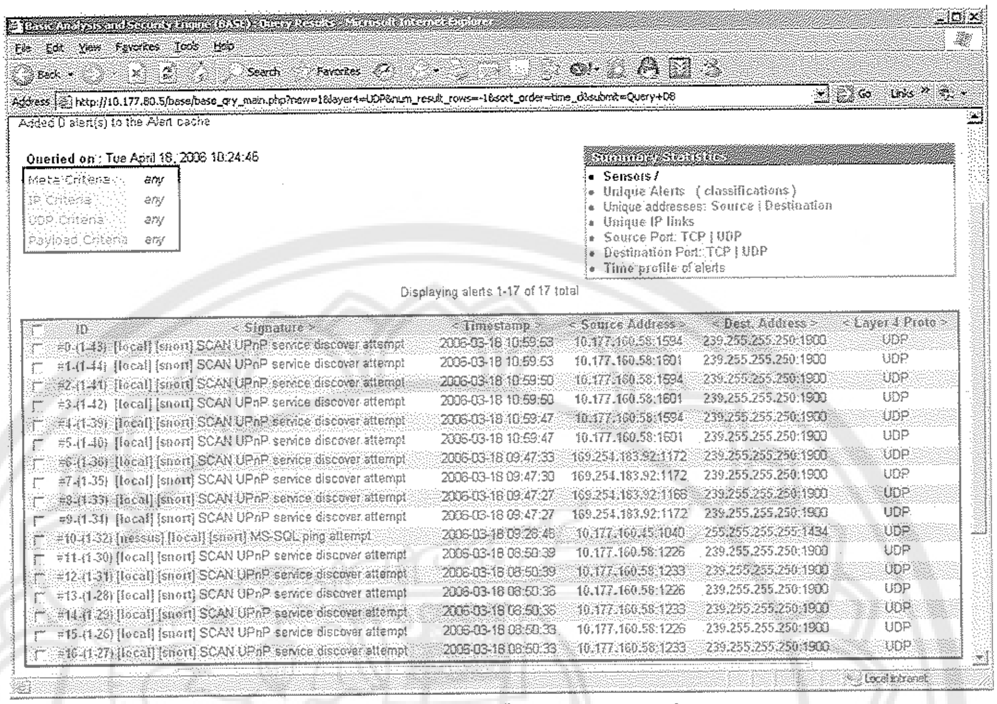


ภาพ 64 หน้าต่างหลักภาควิชาวิทยาแสดงการตรวจจับแพ็กเก็ต

---

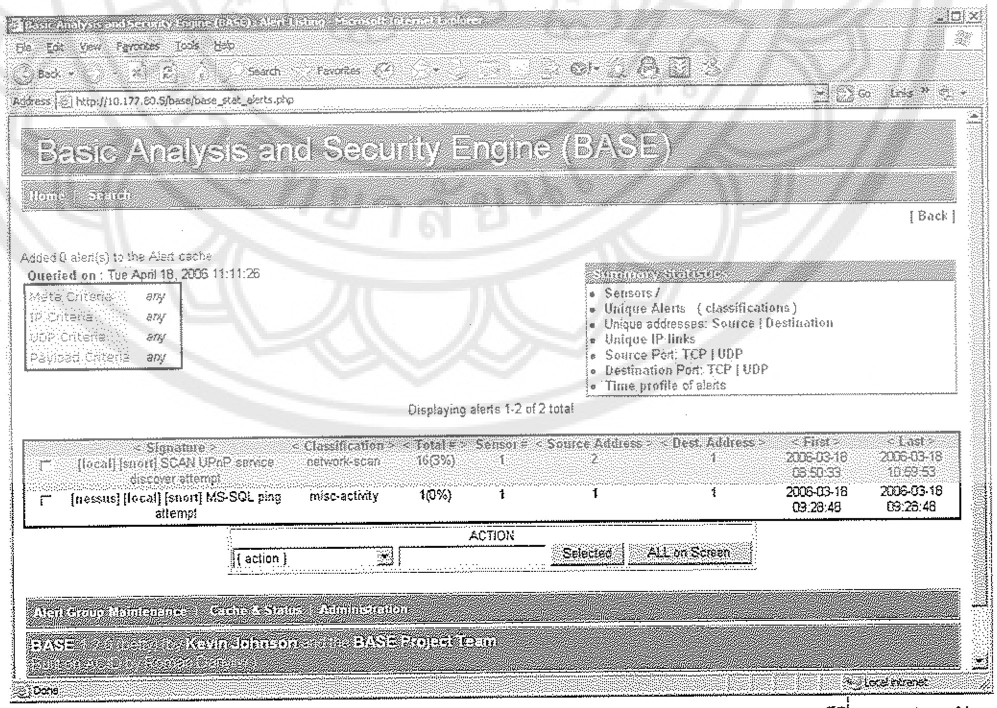
[4] http://www.snort.org/pub-bin/sigs.cgi?sid=466

2.1. โปโตคอล UDP มีการแจ้งเตือนภัย 2 %



ภาพ 65 แสดงการการแจ้งเตือนภัยของโปรโตคอล UDP

แบ่งแยกตามเหตุการณ์ที่สามารถตรวจจับการบุกรุกได้ ดังต่อไปนี้



ภาพ 66 แสดงการเตือนภัยของโปรโตคอล UDP แยกออกตามเหตุการณ์ที่แตกต่างกัน

(Unique Alerts)

2.1.1. เหตุการณ์ที่ 1 เป็นการแจ้งเตือนภัยที่มีข้อความแจ้งว่า "SCAN UPnP service discover attempt" ทั้งหมด 16 ครั้ง

Displaying alerts 1-16 of 16 total

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#0-(1-26)	[local] [snort] SCAN UPnP service discover attempt	2006-03-18 08:50:33	10.177.160.58:1226	239.255.255.250:1900	UDP
#1-(1-27)	[local] [snort] SCAN UPnP service discover attempt	2006-03-18 08:50:33	10.177.160.58:1233	239.255.255.250:1900	UDP
#2-(1-28)	[local] [snort] SCAN UPnP service discover attempt	2006-03-18 08:50:36	10.177.160.58:1226	239.255.255.250:1900	UDP
#3-(1-29)	[local] [snort] SCAN UPnP service discover attempt	2006-03-18 08:50:36	10.177.160.58:1233	239.255.255.250:1900	UDP
#4-(1-30)	[local] [snort] SCAN UPnP service discover attempt	2006-03-18 08:50:39	10.177.160.58:1226	239.255.255.250:1900	UDP
#5-(1-31)	[local] [snort] SCAN UPnP service discover attempt	2006-03-18 08:50:39	10.177.160.58:1233	239.255.255.250:1900	UDP
#6-(1-33)	[local] [snort] SCAN UPnP service discover attempt	2006-03-18 09:47:27	169.254.183.92:1168	239.255.255.250:1900	UDP
#7-(1-34)	[local] [snort] SCAN UPnP service discover attempt	2006-03-18 09:47:27	169.254.183.92:1172	239.255.255.250:1900	UDP
#8-(1-35)	[local] [snort] SCAN UPnP service discover attempt	2006-03-18 09:47:30	169.254.183.92:1172	239.255.255.250:1900	UDP
#9-(1-36)	[local] [snort] SCAN UPnP service discover attempt	2006-03-18 09:47:33	169.254.183.92:1172	239.255.255.250:1900	UDP
#10-(1-39)	[local] [snort] SCAN UPnP service discover attempt	2006-03-18 10:59:47	10.177.160.58:1594	239.255.255.250:1900	UDP
#11-(1-40)	[local] [snort] SCAN UPnP service discover attempt	2006-03-18 10:59:47	10.177.160.58:1601	239.255.255.250:1900	UDP
#12-(1-41)	[local] [snort] SCAN UPnP service discover attempt	2006-03-18 10:59:50	10.177.160.58:1594	239.255.255.250:1900	UDP
#13-(1-42)	[local] [snort] SCAN UPnP service discover attempt	2006-03-18 10:59:50	10.177.160.58:1601	239.255.255.250:1900	UDP
#14-(1-43)	[local] [snort] SCAN UPnP service discover attempt	2006-03-18 10:59:53	10.177.160.58:1594	239.255.255.250:1900	UDP
#15-(1-44)	[local] [snort] SCAN UPnP service discover attempt	2006-03-18 10:59:53	10.177.160.58:1601	239.255.255.250:1900	UDP

ภาพ 67 แสดงการการแจ้งเตือนภัยแบบ SCAN UPnP service discover attempt

คำอธิบาย

เป็นช่วงโหว่ The Universal Plug and Play (UPnP) สามารถย้อนไปอ่านรายละเอียดได้ที่ใน หน้าที่ 10 – 10

ถือเป็นการแจ้งเตือนภัยที่เป็นแบบ True Positive

2.1.2. เหตุการณ์ที่ 2 เป็นการแจ้งเตือนภัยที่มีข้อความแจ้งว่า "MS-SQL ping attempt" ทั้งหมด 1 ครั้ง

Displaying alerts 1-1 of 1 total

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#0-(1-32)	[nessus] [local] [snort] MS-SQL ping attempt	2006-03-18 09:28:48	10.177.160.45:1040	255.255.255.255:1434	UDP

ภาพ 68 แสดงการการแจ้งเตือนภัยแบบ MS-SQL ping attempt

"MS-SQL ping attempt" เป็นเหตุการณ์ที่สามารถอธิบายได้ดังข้อความข้างล่างต่อไปนี้

MS-SQL ping attempt เป็นช่องโหว่สำคัญของระบบปฏิบัติการ Windows นั้นคือ W3 Microsoft SQL Server

[5]W3 Microsoft SQL Server

W3.1คำอธิบาย

Microsoft SQL Server (MSSQL) ประกอบด้วยช่องโหว่อันตรายมากมายที่สามารถช่วยให้ ้ผู้โจมตีขโมยข้อมูลสำคัญ เปลี่ยนแปลงข้อมูลในฐานข้อมูล ทำลายระบบเซิร์ฟเวอร์ SQL และค่าต่างๆ ที่ตั้งไว้ และทำลายเครื่องเซิร์ฟเวอร์ได้

ถึงแม้จะได้มีการเผยแพร่ให้สาธารณชนได้ทราบถึงช่องโหว่ของ MSSQL เหล่านี้แล้ว แต่ก็ยังมีการโจมตีช่องโหว่เหล่านี้ได้สำเร็จอยู่เสมอ แม้กระทั่งหนอน MSSQL ล่าสุดที่แพร่ระบาดในเดือนพฤษภาคม พ.ศ. 2545 ก็ใช้ช่องโหว่ของ MSSQL หลากหลายชนิดที่เป็นที่รู้จักทั่วไป เครื่องต่างๆที่ถูกโจมตีด้วยหนอนชนิดนี้ได้ทำให้การรับ/ส่งข้อมูลทางเครือข่ายเกิดความเสียหายเมื่อเครื่องเหล่านั้นทำการสแกนหาเครื่องอื่นๆ ที่มีช่องโหว่นี้

Internet Storm Center ได้บันทึกไว้ว่า พอร์ต 1433 (พอร์ตที่ MSSQL ใช้โดยอัตโนมัติ) เป็นหนึ่งในหลายๆ พอร์ตที่ถูกสแกนบ่อยที่สุด สามารถดูรายละเอียดเพิ่มเติมในส่วนของ MSSQL นี้ได้จาก CERT ผู้โจมตีสามารถฉวยโอกาสโดยใช้ SQLSnake จากการที่ชื่อบัญชีของผู้ดูแลระบบที่ถูกตั้งมาโดยอัตโนมัติ(ชื่อบัญชี"sa")ไม่มีรหัสผ่าน

ดังนั้นจึงมีความจำเป็นที่จะต้องตั้งค่าให้เหมาะสมและปกป้องระบบใดๆ ให้เชื่อมั่นได้ว่าชื่อบัญชีและรหัสผ่านทั้งหมดของระบบได้รับการปกป้องหรือยกเลิกการใช้งานโดยสมบูรณ์กรณีที่ไม่ได้ใช้งาน สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการตั้งค่าและจัดการกับรหัสผ่านของบัญชีชื่อ sa สามารถศึกษาได้จากเอกสาร Microsoft Developer Network เรื่อง Changing the SQL Server Administrator Login และ Verify and Change the System Administrator Password by Using MSDE บัญชีชื่อ sa ควรจะมีรหัสผ่านที่ง่ายต่อการจำแต่ยากต่อการเดา ถึงแม้ว่าจะไม่ได้ใช้ในการทำงานของ SQL/MSDE ก็ตาม

ผู้โจมตีสามารถฉวยโอกาสโดยใช้ SQL Slammer จากการล้นของบัฟเฟอร์ของบริการ SQL Server Resolution เมื่อหนอนส่งแพ็กเก็ตโจมตีไปที่พอร์ต 1434/UDP ของเครื่องที่เป็นเป้าหมายซึ่งมีช่องโหว่อยู่จะทำให้บัฟเฟอร์ล้นและความปลอดภัยของเครื่องลดลง ถ้าเครื่องใดๆ เปิดบริการ

---

5 ศิริวรรณ อภิสิริเดช และ มนัชยา ชมธวัช , 20 ช่องโหว่สำคัญที่เป็นอันตรายร้ายแรงต่อความปลอดภัยของอินเทอร์เน็ต, http://www.thaicert.nectec.or.th/paper/basic/top20.php#W3

SQL อยู่ก็มีความเสี่ยงที่จะเกิดการล้นของหน่วยความจำและได้รับแพ็กเก็ตดังกล่าว ซึ่งจะทำให้เกิดความเสียหายต่อระบบความปลอดภัยทั้งหมดของระบบและเซิร์ฟเวอร์ การป้องกันที่ดีที่สุดจากผลกระทบของหนอนชนิดนี้ที่ดีที่สุดคือการติดตั้ง patch หมั่นตั้งค่าระบบในการป้องกัน และกรองการเข้าออกของแพ็คเก็ตผ่านพอร์ต 1434/UDP ที่ทางออกของเครือข่ายที่เชื่อมไปสู่เครือข่ายภายนอก

เราอาจกล่าวได้ว่า Microsoft Server 2000 Desktop Engine (MSDE 2000) เป็นเซิร์ฟเวอร์ SQL กลายๆ ตัวหนึ่ง ("SQL Server Lite")
เจ้าของระบบหลายคน ไม่ได้ตระหนักว่าระบบ มี MSDE ทำงานอยู่ และมี SQL Server ติดตั้งอยู่ อนึ่ง MSDE 2000 นั้น ถูกติดตั้งไว้เป็นส่วนหนึ่งของผลิตภัณฑ์ของ Microsoft ต่างๆ ดังนี้:

1. SQL/MSDE Server 2000 (Developer, Standard and Enterprise Editions)
2. Visual Studio .NET (Architect, Developer and Professional Editions)
3. ASP.NET Web Matrix Tool
4. Office XP
5. Access 2002
6. Visual Fox Pro 7.0/8.0

W3.4 **วิธีการตรวจสอบว่า ได้รับผลกระทบจากช่องโหว่นี้หรือไม่**
บริษัท Microsoft ได้เผยแพร่เครื่องมือด้านความปลอดภัยไว้ที่
http://www.microsoft.com/sql/downloads/securitytools.asp สำหรับ toolkit ชื่อ SQL Critical Update Kit ประกอบด้วยเครื่องมือที่มีประโยชน์มากมายเช่น SQL Scan, SQL Check, and SQL Critical Update

Chip Andrews จาก sqlsecurity.com ได้เผยแพร่เครื่องมือชื่อ SQLPingv2.2 เครื่องมือนี้จะส่งแพ็กเก็ต UDP แบบไบต์เดี่ยว (ค่าไบต์เป็น 0x02) ไปยังพอร์ต 1434 ของเครื่องเดี่ยวหรือไม่ก็ทุกเครื่องในวง subnet ซึ่งจะทำให้เซิร์ฟเวอร์ SQL ที่กำลังรอรับการเชื่อมต่อที่พอร์ต 1434/UDP นั้นตอบสนองโดยการเปิดเผยรายละเอียดของระบบเช่น หมายเลขเวอร์ชัน ค่าต่างๆ เป็นต้น เครื่องมือ SQLPingv2.2 เป็นเครื่องมือสำหรับสแกนและค้นหาซึ่งเหมือนกับ SQL SCan ของ Microsoft ซึ่งจะไม่ละเมิดความปลอดภัยของระบบและเครือข่าย นอกจากนี้ยังมีเครื่องมือเกี่ยวกับความปลอดภัยอยู่ที่ SQL/MSDE Security Web site ของ Chip Andrews ด้วย

W3.5 วิธีการป้องกันอันตรายจากช่องโหว่นี้

โดยสรุป

1. ยกเลิกการทำงานของบริการ SQL/MSDE Monitor บนพอร์ต 1434/UDP
2. ติดตั้ง service pack ล่าสุดสำหรับ Microsoft SQL/MSDE server และ/หรือ MSDE 2000
3. ติดตั้ง cumulative patch ล่าสุดที่เผยแพร่หลังจาก service pack ล่าสุด
4. ติดตั้ง patch แต่ละตัวที่เผยแพร่ออกมาหลังจาก cumulative patch ล่าสุด
5. เก็บบันทึกการพิสูจน์ตัวตนบนเครื่องเซิร์ฟเวอร์ SQL
6. รักษาความปลอดภัยเครื่องเซิร์ฟเวอร์ทั้งระดับระบบและระดับเครือข่าย
7. ลดระดับสิทธิของบริการ MSSQL/MSDEServer และ SQL/MSDE Server Agent

รายละเอียด

1. ยกเลิกการทำงานของบริการ SQL/MSDE Monitor บนพอร์ต 1434/UDP

สามารถทำได้โดยการติดตั้งและใช้ฟังก์ชันภายใน SQLServer2000 ServicePack3a Microsoft's database engine MSDE 2000 มีช่องโหว่จากการล้นของบัฟเฟอร์ซึ่งผู้โจมตีจากภายนอกสามารถฉวยโอกาสได้โดยไม่ต้องทำการพิสูจน์ตัวตนกับเครื่องเซิร์ฟเวอร์เลย การโจมตีแบบนี้อาศัยช่องทางของ UDP ไม่ว่ากระบวนการ MSDE 2000 จะทำงานในระบบความปลอดภัยของ domain user หรือบัญชี SYSTEM ของเครื่อง การโจมตีช่องโหว่นี้ถือว่าเป็นการบุกรุกระบบเป้าหมายโดยสมบูรณ์ หนอน MS-SQL/MSDE Slammer ส่ง แพ็กเก็ตที่มีขนาด 376 ไบต์ไปยังพอร์ต 1434 โดยใช้การสุ่มเป้าหมายด้วยอัตราเร็วสูงมาก ระบบที่ถูกโจมตีจะเริ่มส่งแพ็กเก็ตขนาด 376 ไบต์ทันทีที่ติดเชื้อหนอนชนิดนี้ หนอนจะส่งข้อมูลจำนวนมากไปยังหมายเลข IP ที่สุ่มขึ้นมารวมทั้ง IP แบบ multicast ทำให้เครือข่ายเป้าหมายไม่สามารถให้บริการได้ (Denial of Service) อีกต่อไป มีการรายงานว่าเครื่องเครื่องหนึ่งที่ได้รับเชื้อนี้สร้างข้อมูลออกมาในอัตราที่มากกว่า 50 Mb/sec

2. ติดตั้ง service pack สำหรับ Microsoft SQL server สำหรับ Microsoft SQL Server service pack เวอร์ชันล่าสุดคือ

- SQL/MSDE Server 7.0 Service Pack 4
- MSDE/SQL Server 2000 Service Pack 3a

เพื่อติดตามการอัพเกรดต่อไปอย่างใกล้ชิด ควรตรวจดูที่ Make Your SQL/MSDE Servers Less Vulnerable จาก Microsoft Technet

3. ติดตั้ง cumulative patch ล่าสุดที่เผยแพร่หลังจาก service pack ล่าสุด

สามารถดาวน์โหลด cumulative patch สำหรับ SQL Server ทุกเวอร์ชันได้ที่ MS02-061 Elevation of Privilege in SQL/MSDE Server Web Tasks (Q316333/Q327068)

เพื่อติดตามการอัพเกรดต่อไปอย่างใกล้ชิด ควรตรวจดู cummulative patch ที่:

- Microsoft SQL/MSDE Server 7.0
- Microsoft SQL Server 2000
- MSDE Server Desktop Engine 2000 (MSDE 2000)

4. ติดตั้ง patch แต่ละอย่างที่เผยแพร่ออกมาหลังจาก cumulative patch ล่าสุด

ปัจจุบันไม่มี patch เผยแพร่ออกมาหลังจากการเผยแพร่การอัพเกรดของ MS02 -061 Elevation of Privilege in SQL/MSDE Server Web Tasks (Q316333/Q327068) แต่เพื่อติดตามการอัพเกรดต่อไปอย่างใกล้ชิด ควรตรวจดู patch แต่ละชนิดที่เผยแพร่ออกมาที่

- Microsoft SQL/MSDE Server 7.0
- Microsoft SQL Server 2000
- MSDE Server Desktop Engine 2000 (MSDE 2000)

5. เก็บบันทึกการพิสูจน์ตัวตนบนเครื่องเซิร์ฟเวอร์ SQL

เปิดให้มีการเก็บบันทึกการพิสูจน์ตัวตนบนเซิร์ฟเวอร์ SQL (ตามปกติจะไม่ได้เปิดไว้) วิธีนี้สามารถทำได้โดยผ่าน Enterprise Manager (Server properties; tab Security)

6. รักษาความปลอดภัยเครื่องเซิร์ฟเวอร์ทั้งระดับระบบและระดับเครือข่าย

จุดอ่อนจุดหนึ่งของ MSSQL ที่มักถูกโจมตีคือ ชื่อบัญชีของผู้ดูแลระบบที่ตั้งมาโดยอัตโนมัติ (คือ "sa") จะไม่มีรหัสผ่าน ถ้าชื่อบัญชี "sa" ของ SQL ไม่ได้รับการปกป้องด้วยรหัสผ่าน ถือว่าระบบไม่มี

ความปลอดภัยและอาจถูกโจมตีโดยหนอนอินเทอร์เน็ต และการโจมตีแบบอื่นๆ ดังนั้นควรปฏิบัติตามคำแนะนำจากหัวข้อ "System Administraor (SA) login" ใน SQL/MSDE Server Books Online เพื่อทำให้ชื่อบัญชี "sa" ที่มากับระบบมีรหัสผ่านที่แข็งแรง แม้ว่า SQL Server จะไม่ได้ทำงานด้วยชื่อบัญชีนี้ก็ตาม

มีเอกสารเกี่ยวกับระบบเครือข่ายของ Microsoft Developer ที่ การเปลี่ยน SQL Server Administrator Login และวิธีตรวจสอบและเปลี่ยนรหัสผ่านของผู้ดูแลระบบโดยใช้ MSDE

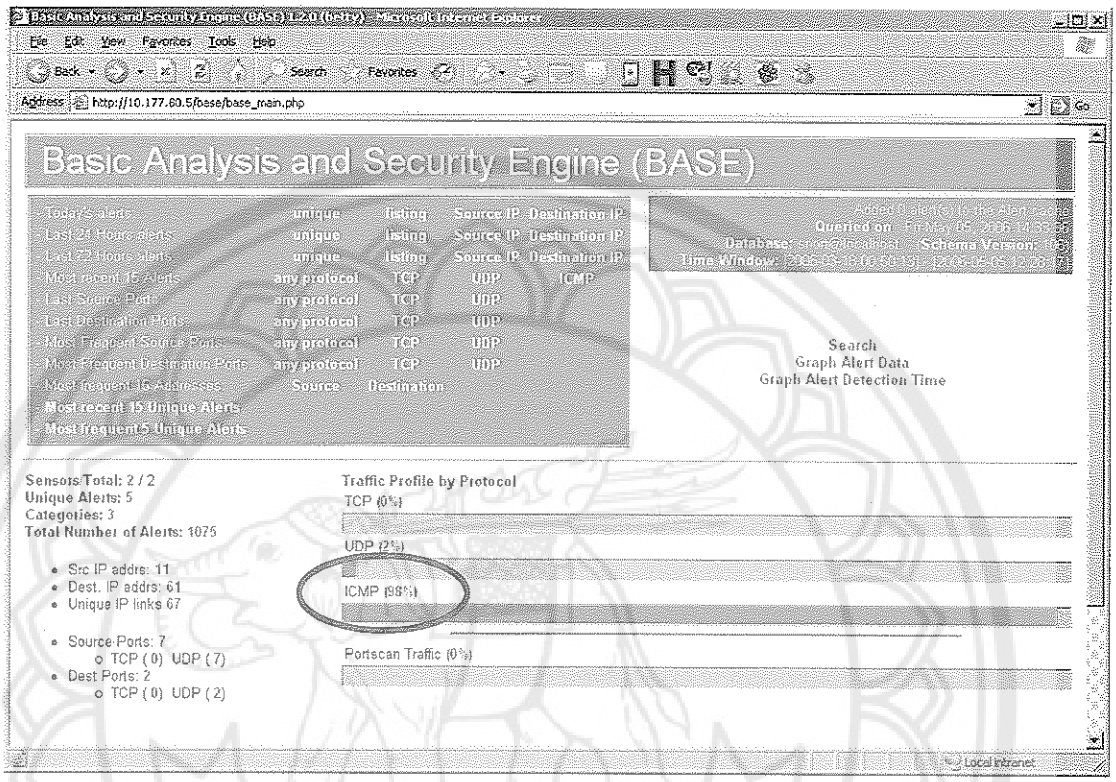
7. ลดระดับสิทธิของบริการ MSSQL/MSDEServer และ SQL/MSDE Server Agent

เปิดบริการ MSSQL/MSDES Server และ SQL/MSDE Server Agent ภายใต้ชื่อบัญชีของโดเมนที่ใช้ได้ (valid domain account) ด้วยสิทธิที่น้อยที่สุดที่จะยอมให้มีการเปิดบริการได้ และต้องไม่เป็นชื่อบัญชีของผู้ดูแลโดเมนหรือ SYSTEM (บน NT) หรือ LocalSystem (บน Windows 2000 หรือ XP) หากมีการเปิดบริการโดยใช้ชื่อบัญชีที่มีสิทธิพิเศษดังกล่าวข้างต้นในระดับ local หรือโดเมน จะทำให้ผู้โจมตีสามารถควบคุมเครื่องและ/หรือเครือข่ายได้อย่างสมบูรณ์

1. เปิดใช้ WindowsNT Authentication คือการเปิดใช้การตรวจสอบการล็อกอินเข้าสู่ระบบทั้งที่สำเร็จและไม่สำเร็จ แล้วหยุดและเริ่มบริการ MSSQL Server ใหม่ ตั้งค่าการทำงานของเครื่องลูกข่ายให้ใช้ NT Authentication ด้วย
2. ควรให้มีการกรองแพ็คเก็ตบริเวณขอบของเครือข่ายเพื่อป้องกันการเชื่อมต่อจากภายนอกมาใช้บริการโดยไม่ได้รับอนุญาต การกรองข้อมูลขาเข้าของ TCP port 1433 และ 1434 สามารถป้องกันผู้โจมตีจากภายนอกเครือข่ายที่จะมาสแกนหรือโจมตีช่องโหว่ของ Microsoft SQL servers ในเครือข่ายภายในซึ่งไม่อนุญาตในการให้บริการ SQL สู่ภายนอก
3. ถ้าจำเป็นต้องเปิดใช้พอร์ต 1433/TCP และ 1434/TCP ที่ Internet gateways ให้เปิดใช้และตั้งค่าการกรองแพ็คเก็ตขาเข้า/ขาออก ให้รัดกุมที่สุดเพื่อป้องกันการใช้พอร์ตนี้ในทางที่ผิด

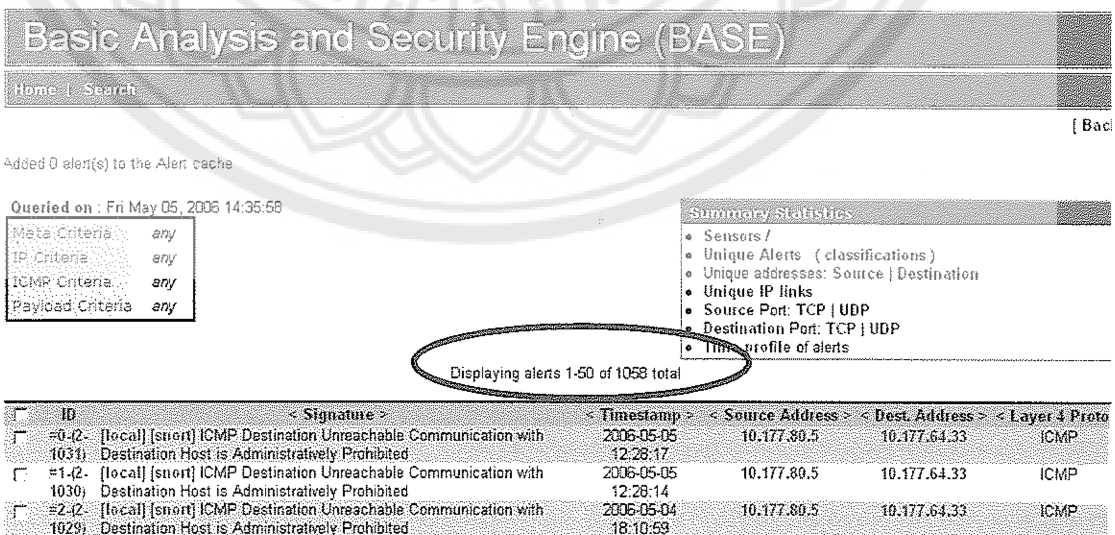
ถือเป็นการแจ้งเตือนภัยที่เป็นแบบ True Positive

2.2. โปโตคอล ICMP มีการแจ้งเตือนภัย 98 %



ภาพ 69 แสดงการแจ้งเตือนภัยโปโตคอล ICMP 98%

มีการแจ้งเตือนภัยจำนวน 1058 ครั้งดังรูป



ภาพ 70 แสดงการแจ้งเตือนภัยโปโตคอล ICMP จำนวน 1058 ครั้ง

แบ่งแยกตามเหตุการณ์ที่สามารถตรวจจับการบุกรุกได้ ดังต่อไปนี้

[Back

Added 0 alert(s) to the Alert cache

Queried on : Fri May 05, 2006 14:39:31

Meta Criteria	*any*
IP Criteria	*any*
ICMP Criteria	*any*
Payload Criteria	*any*

Summary Statistics

- Sensors /
- Unique Alerts (classifications)
- Unique addresses: Source | Destination
- Unique IP links
- Source Port: TCP | UDP
- Destination Port: TCP | UDP
- Time profile of alerts

Displaying alerts 1-3 of 3 total

< Signature >	< Classification >	< Total # >	Sensor #	< Source Address >	< Dest. Address >	< First >	< Last >
[local] [snort] ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	misc-activity	1042(97%)	2	2	50	2006-03-18 00:50:13	2006-05-05 12:28:17
[arachNIDS] [local] [snort] ICMP L3retriever Ping	attempted-recon	11(1%)	1	4	8	2006-03-22 11:47:14	2006-05-01 13:54:09
[arachNIDS] [local] [snort] ICMP PING NMAP	attempted-recon	5(0%)	1	2	1	2006-04-20 23:59:22	2006-05-03 09:56:43

ภาพ 71 แสดงเหตุการณ์ของการแจ้งเตือนภัยโปโตคอล ICMP (Unique Alerts)

2.2.1 เหตุการณ์ "ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited " จำนวนทั้งสิ้น 1042 ครั้ง

< Signature >	< Classification >	< Total # >	Sensor #	< Source Address >	< Dest. Address >	< First >	< Last >
[local] [snort] ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	misc-activity	1042(97%)	2	2	50	2006-03-18 00:50:13	2006-05-0 12:28:17

ภาพ 72 แสดงเหตุการณ์ของการแจ้งเตือนภัยโปโตคอล ICMP "ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited "

"ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited " เป็นเหตุการณ์ที่สามารถอธิบายได้ดังข้อความข้างล่างต่อไปนี้

คำอธิบาย

ICMP ชนิดไม่สามารถติดต่อสถานีปลายทาง

เป็นการแจ้งเตือนภัยเกี่ยวกับการป้องกันการโจมตีที่เกิดขึ้นแบบ Denial of Service ซึ่งหาก router ไม่สามารถส่ง datagram ไปยัง router หรือ host ถัดไปได้ router จะตอบกลับด้วย ICMP และใส่รหัสในฟิลด์ code เพื่อบอกสาเหตุของปัญหา

0 – 7	8 – 15	16 – 31
Type = 3	Code = 0 – 15	Checksum
ไม่ใช้งาน (มีค่าเป็น 0)		
Header IP + 64 bit แรกของข้อมูล		

ภาพ 73 ICMP datagram

Code	ความผิดพลาด	ความหมาย
0	Network unreachable	ไปไม่ถึงเครือข่าย
1	Host unreachable	ไปไม่ถึง host
2	Protocol unreachable	ไปไม่ถึง protocol ปลายทาง
3	Port unreachable	ไปไม่ถึง port
4	Fragmentation needed but the Do Not Fragment bit was set	จำเป็นต้องแบ่ง datagram แต่มีการกำหนดไม่ให้แบ่งแยก
5	Source route failed	เส้นทางที่กำหนดล้มเหลว
6	Destination network unknown	ไม่ปรากฏเครือข่ายปลายทาง
7	Destination host unknown	ไม่ปรากฏ host ปลายทาง
8	Source host isolated (obsolete)	
9	Destination network administratively prohibited	มีการป้องกันไม่ให้เข้าเครือข่ายปลายทาง
10	Destination host administratively prohibited	มีการป้องกันไม่ให้เข้า host ปลายทาง

ภาพ 74 Code ของ ICMP

ถือเป็นการแจ้งเตือนภัยที่เป็นแบบ True Positive

2.2.2 เหตุการณ์ "ICMP L3retriever Ping" จำนวนทั้งสิ้น 11 ครั้ง

	< Signature >	< Classification >	< Total # >	Sensor #	< Source Address >	< Dest. Address >	< First >	< Last >
☐	[arachNIDS] [local] [snort] ICMP L3retriever Ping	attempted-recon	11(1%)	1	4	8	2006-03-22 11:47:14	2006-05-01 13:54:09

ภาพ 75 แสดงเหตุการณ์ของการแจ้งเตือนภัยโปโตคอล ICMP "ICMP L3retriever Ping"

เป็นข้อความแจ้งเตือนภัยของ [6]ICMP echo request จากเครื่องที่ใช้ L3 "Retriever 1.5" ในการสแกน

---

6 http://www.snort.org/pub-bin/sigs.cgi?sid=466

2.2.3 เหตุการณ์ "ICMP PING NMAP" จำนวนทั้งสิ้น 1 ครั้ง

< Signature >	< Classification >	< Total # >	Sensor #	< Source Address >	< Dest. Address >	< First >	< Last >
[arachNIDS] [local] [snort] ICMP PING NMAP	attempted-recon	5(0%)	1	2	1	2006-04-20 23:59:22	2006-05-03 09:56:43

ภาพ 76 แสดงเหตุการณ์ของการแจ้งเตือนภัยโปโตคอล ICMP "ICMP PING NMAP"

เหตุการณ์ "ICMP PING NMAP" เป็นเหตุการณ์ที่สามารถอธิบายได้ดังข้อความข้างล่างต่อไปนี้ เป็นการแจ้งเตือนภัยจากการโดน Port scanning ด้วยโปรแกรม NMAP

Displaying alerts 1-5 of 5 total

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#0-(2-571)	[arachNIDS] [local] [snort] ICMP PING NMAP	2006-04-20 23:59:22	10.177.64.33	10.177.80.5	ICMP
#1-(2-793)	[arachNIDS] [local] [snort] ICMP PING NMAP	2006-04-26 11:03:00	10.177.64.105	10.177.80.5	ICMP
#2-(2-938)	[arachNIDS] [local] [snort] ICMP PING NMAP	2006-05-02 09:35:47	10.177.64.105	10.177.80.5	ICMP
#3-(2-958)	[arachNIDS] [local] [snort] ICMP PING NMAP	2006-05-02 17:58:26	10.177.64.33	10.177.80.5	ICMP
#4-(2-968)	[arachNIDS] [local] [snort] ICMP PING NMAP	2006-05-03 09:55:43	10.177.64.105	10.177.80.5	ICMP

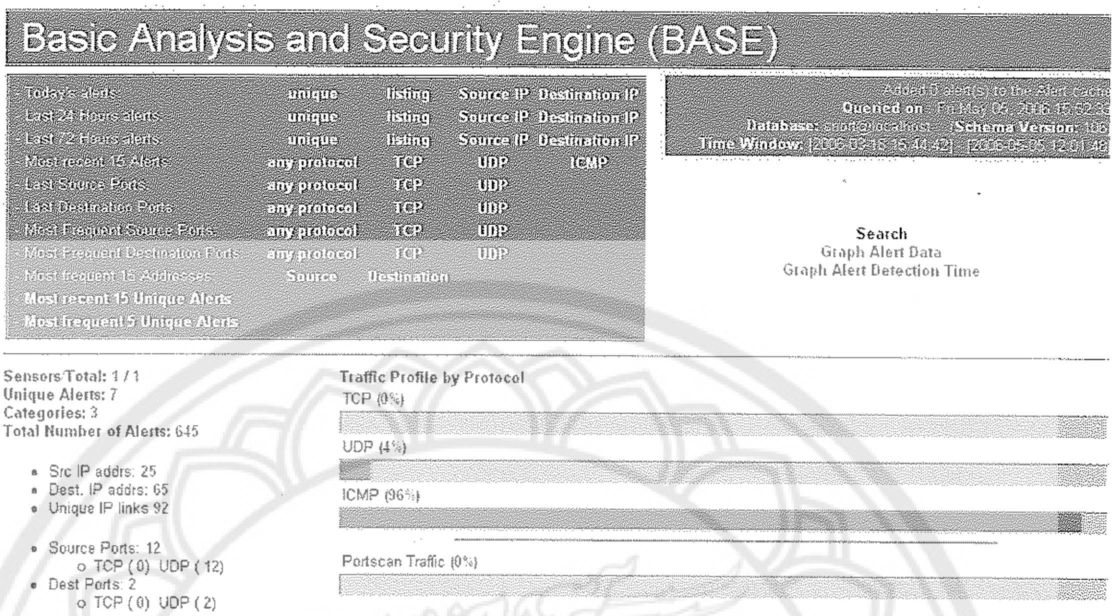
ภาพ 77 แสดงเหตุการณ์ของการแจ้งเตือนภัยโปโตคอล ICMP "ICMP PING NMAP" ตามหมายเลขไอพีต้นทางไปยังหมายเลขไอพีปลายทาง

ถือเป็นการแจ้งเตือนภัยที่เป็นแบบ True Positive

3. ภาควิชาเคมี

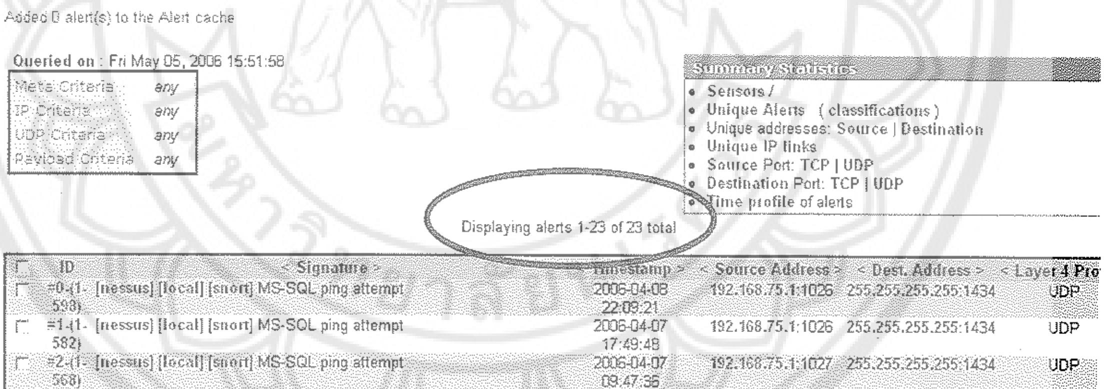
การตรวจจับออกเป็นสัดส่วนได้ดังต่อไปนี้

- โปโตคอล TCP มีการแจ้งเตือนภัย 0 %
- โปโตคอล UDP มีการแจ้งเตือนภัย 4 %
- โปโตคอล ICMP มีการแจ้งเตือนภัย 96 %
- Portscan Traffic มีการแจ้งเตือนภัย 0 %



ภาพ 78 หน้าต่างหลักภาควิชาเคมีแสดงการตรวจจับแพ็กเก็ต

3.1 โปโตคอล UDP มีการแจ้งเตือนภัย 4 %เป็นจำนวนทั้งสิ้น 23 ครั้ง



ภาพ 79 แสดงการแจ้งเตือนภัยโปรโตคอล UDP จำนวนทั้งหมด 23 ครั้ง

แบ่งแยกตามเหตุการณ์ที่สามารถตรวจจับการบุกรุกได้ ดังต่อไปนี้

[Bacl

Added 0 alert(s) to the Alert cache

Queried on : Fri May 05, 2006 15:54:52

Meta Criteria	*any*
IP Criteria	*any*
UDP Criteria	*any*
Payload Criteria	*any*

Summary Statistics

- **Sensors /**
- **Unique Alerts (classifications)**
- **Unique addresses: Source | Destination**
- **Unique IP links**
- Source Port: TCP | UDP
- Destination Port: TCP | UDP
- Time profile of alerts

Displaying alerts 1-4 of 4 total

< Signature >	< Classification >	< Total # >	Sensor #	< Source Address >	< Dest. Address >	< First >	< Last >
[nessus] [local] [snort] MS-SQL ping attempt	misc-activity	15(2%)	1	4	1	2006-03-26 16:21:07	2006-04-0 22:09:21
[cve] [icat] [cve] [icat] [cve] [icat] [bugtraq] [bugtraq] [bugtraq] [local] [snort] SNMP public access udp	attempted-recon	2(0%)	1	1	1	2006-04-04 14:56:20	2006-04-0 14:56:21
[cve] [icat] [cve] [icat] [bugtraq] [bugtraq] [bugtraq] [local] [snort] SNMP request udp	attempted-recon	3(0%)	1	1	1	2006-04-04 14:56:20	2006-04-0 14:56:21
[cve] [icat] [cve] [icat] [bugtraq] [bugtraq] [bugtraq] [local] [snort] SNMP Broadcast request	attempted-recon	3(0%)	1	1	1	2006-04-04 14:56:20	2006-04-0 14:56:21

ภาพ 80 แสดงการแจ้งเตือนภัยโปรโตคอล UDP แบ่งแยกตามเหตุการณ์

ซึ่งแบ่งออกได้ 4 เหตุการณ์

3.1.1 เหตุการณ์ที่ 1 เป็นการแจ้งเตือนภัยที่มีข้อความแจ้งว่า “MS-SQL ping attempt” ทั้งหมด 15 ครั้ง

Displaying alerts 1-15 of 15 total

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#0-(1-217)	[nessus] [local] [snort] MS-SQL ping attempt	2006-03-26 16:21:07	192.168.0.1:3010	255.255.255.255:1434	UDP
#1-(1-318)	[nessus] [local] [snort] MS-SQL ping attempt	2006-03-29 23:25:06	10.177.32.51:3011	255.255.255.255:1434	UDP
#2-(1-528)	[nessus] [local] [snort] MS-SQL ping attempt	2006-04-06 00:18:34	10.177.32.40:1135	255.255.255.255:1434	UDP
#3-(1-529)	[nessus] [local] [snort] MS-SQL ping attempt	2006-04-06 01:32:06	10.177.32.40:1340	255.255.255.255:1434	UDP
#4-(1-530)	[nessus] [local] [snort] MS-SQL ping attempt	2006-04-06 01:34:09	10.177.32.40:1341	255.255.255.255:1434	UDP
#5-(1-531)	[nessus] [local] [snort] MS-SQL ping attempt	2006-04-06 01:34:12	10.177.32.40:1342	255.255.255.255:1434	UDP
#6-(1-532)	[nessus] [local] [snort] MS-SQL ping attempt	2006-04-06 02:01:05	192.168.75.1:1037	255.255.255.255:1434	UDP
#7-(1-533)	[nessus] [local] [snort] MS-SQL ping attempt	2006-04-06 02:43:01	192.168.75.1:1026	255.255.255.255:1434	UDP
#8-(1-538)	[nessus] [local] [snort] MS-SQL ping attempt	2006-04-06 13:49:36	192.168.75.1:1040	255.255.255.255:1434	UDP
#9-(1-544)	[nessus] [local] [snort] MS-SQL ping attempt	2006-04-06 14:31:17	192.168.75.1:1026	255.255.255.255:1434	UDP
#10-(1-545)	[nessus] [local] [snort] MS-SQL ping attempt	2006-04-06 16:34:16	192.168.75.1:1027	255.255.255.255:1434	UDP
#11-(1-550)	[nessus] [local] [snort] MS-SQL ping attempt	2006-04-07 00:10:58	192.168.75.1:1025	255.255.255.255:1434	UDP
#12-(1-568)	[nessus] [local] [snort] MS-SQL ping attempt	2006-04-07 09:47:36	192.168.75.1:1027	255.255.255.255:1434	UDP
#13-(1-582)	[nessus] [local] [snort] MS-SQL ping attempt	2006-04-07 17:49:48	192.168.75.1:1026	255.255.255.255:1434	UDP
#14-(1-598)	[nessus] [local] [snort] MS-SQL ping attempt	2006-04-08 22:09:21	192.168.75.1:1026	255.255.255.255:1434	UDP

ภาพ 81 แสดงการการแจ้งเตือนภัยแบบ MS-SQL ping attempt

“MS-SQL ping attempt” เป็นเหตุการณ์ที่สามารถอธิบายได้ดังข้อความข้างล่างต่อไปนี้

MS-SQL ping attempt เป็นช่องโหว่สำคัญของระบบปฏิบัติการ Windows นั้นคือ W3 Microsoft SQL Server

คำอธิบาย

เป็นช่วงโหว่ The Universal Plug and Play (UPnP) สามารถย้อนไปอ่านรายละเอียดได้ที่ในหน้าที่ 10 – 17

ถือเป็นการแจ้งเตือนภัยที่เป็นแบบ True Positive

3.1.2 เหตุการณ์ที่ 2 เป็นการแจ้งเตือนภัยที่มีข้อความแจ้งว่า "SNMP public access udp" ทั้งหมด 2 ครั้ง

3.1.3 เหตุการณ์ที่ 3 เป็นการแจ้งเตือนภัยที่มีข้อความแจ้งว่า "SNMP request udp" ทั้งหมด 3 ครั้ง

3.1.4 เหตุการณ์ที่ 4 เป็นการแจ้งเตือนภัยที่มีข้อความแจ้งว่า "SNMP Broadcast request" ทั้งหมด 3 ครั้ง

☐	[cve] [icat] [cve] [icat] [cve] [icat] [bugtraq] [bugtraq] [bugtraq] [local] [snort] SNMP public access udp	attempted-recon	2(0%)	1	1	1	2006-04-04 14:56:20	2006-04-04 14:56:21
☐	[cve] [icat] [cve] [icat] [bugtraq] [bugtraq] [bugtraq] [local] [snort] SNMP request udp	attempted-recon	3(0%)	1	1	1	2006-04-04 14:56:20	2006-04-04 14:56:21
☐	[cve] [icat] [cve] [icat] [bugtraq] [bugtraq] [bugtraq] [local] [snort] SNMP Broadcast request	attempted-recon	3(0%)	1	1	1	2006-04-04 14:56:20	2006-04-04 14:56:21

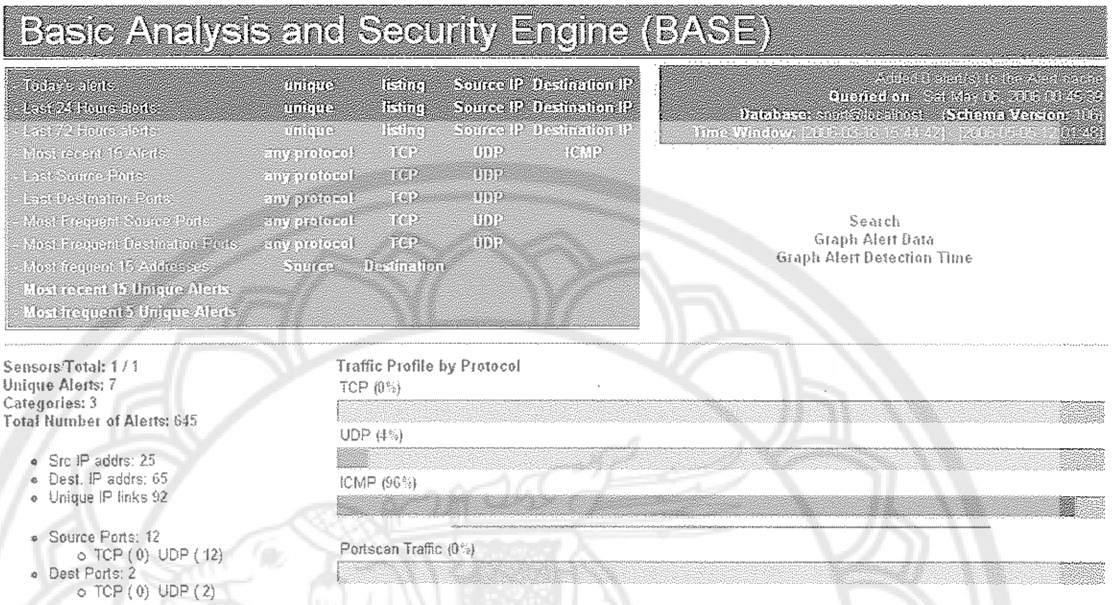
ภาพ 82 การแจ้งเตือนภัยเกี่ยวกับเป็นช่วงโหว่ SNMP Service

คำอธิบาย

เป็นช่วงโหว่ SNMP Service สามารถย้อนไปอ่านรายละเอียดได้ที่ในหน้าที่ 10 – 5

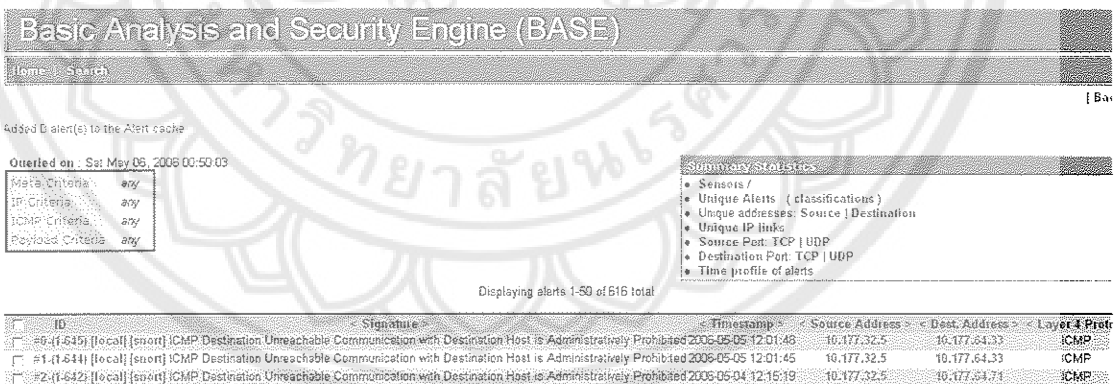
ถือเป็นการแจ้งเตือนภัยที่เป็นแบบ True Positive

3.2 โปรโตคอล ICMP มีการแจ้งเตือนภัย 96 %



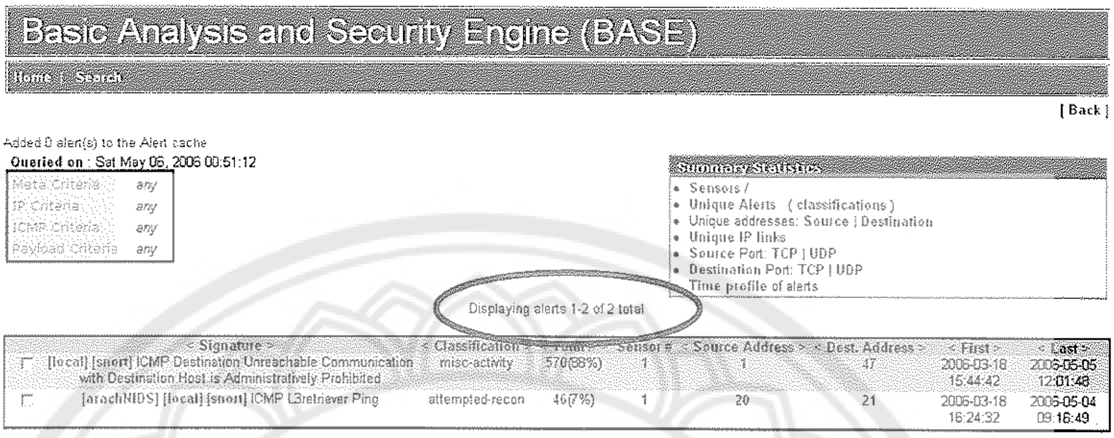
ภาพ 83 แสดงการแจ้งเตือนภัยโปรโตคอล ICMP จำนวน 96 %

เป็นจำนวนทั้งสิ้น 616 ครั้ง



ภาพ 84 แสดงการแจ้งเตือนภัยโปรโตคอล ICMP เป็นจำนวนทั้งสิ้น 616 ครั้ง

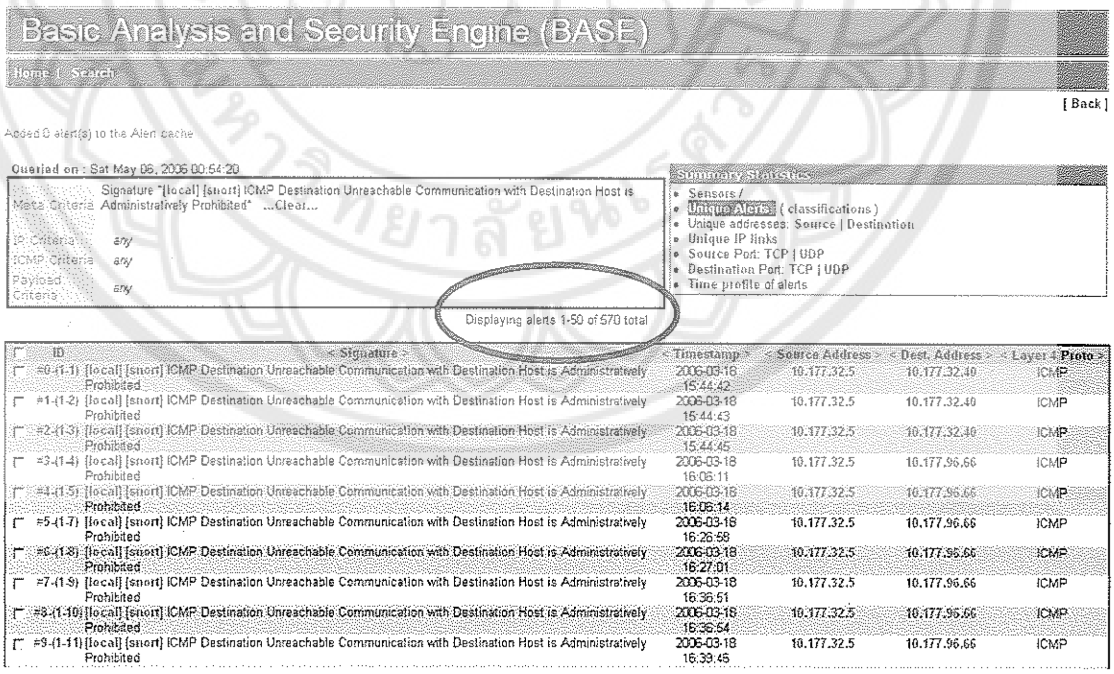
แบ่งแยกตามเหตุการณ์ที่สามารถตรวจจับการบุกรุกได้ ดังต่อไปนี้



ภาพ 85 แสดงการแจ้งเตือนภัยโปรโตคอล ICMP แบ่งแยกตามเหตุการณ์(Unique Alerts)

ซึ่งแบ่งออกได้ 2 เหตุการณ์

3.2.1 เหตุการณ์ที่ 1 "ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited" จำนวนทั้งสิ้น 570 ครั้ง



ภาพ 86 แสดงเหตุการณ์ของการแจ้งเตือนภัยโปโตคอล ICMP "ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited "

"ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited " เป็นเหตุการณ์ที่สามารถอธิบายได้ดังข้อความข้างล่างต่อไปนี้

ICMP ชนิดไม่สามารถติดต่อสถานีปลายทาง

เป็นการแจ้งเตือนภัยเกี่ยวกับการป้องกันการโจมตีที่เกิดขึ้นแบบ Denial of Service ซึ่งหาก router ไม่สามารถส่ง datagram ไปยัง router หรือ host ถัดไปได้ router จะตอบกลับด้วย ICMP และใส่รหัสในฟิลด์ code เพื่อบอกสาเหตุของปัญหา

0 7	8 15	16 31
Type = 3	Code = 0 – 15	Checksum
ไม่ใช้งาน (มีค่าเป็น 0)		
Header IP + 64 bit แรกของข้อมูล		

ภาพ 87 ICMP datagram

Code	ความผิดพลาด	ความหมาย
0	Network unreachable	ไปไม่ถึงเครือข่าย
1	Host unreachable	ไปไม่ถึง host
2	Protocol unreachable	ไปไม่ถึง protocol ปลายทาง
3	Port unreachable	ไปไม่ถึง port
4	Fragmentation needed but the Do Not Fragment bit was set	จำเป็นต้องแบ่ง datagram แต่มีการกำหนดไม่ให้แบ่งแยก
5	Source route failed	เส้นทางที่กำหนดล้มเหลว
6	Destination network unknown	ไม่ปรากฏเครือข่ายปลายทาง
7	Destination host unknown	ไม่ปรากฏ host ปลายทาง
8	Source host isolated (obsolete)	
9	Destination network administratively prohibited	มีการป้องกันไม่ให้เข้าเครือข่ายปลายทาง
10	Destination host administratively prohibited	มีการป้องกันไม่ให้เข้า host ปลายทาง

ภาพ 88 Code ของ ICMP

ถือเป็นการแจ้งเตือนภัยที่เป็นแบบ True Positive

3.2.1 เหตุการณ์ "ICMP L3retriever Ping" จำนวนทั้งสิ้น 46 ครั้ง

< Signature >	< Classification >	< Total # >	Sensor #	< Source Address >	< Dest. Address >	< First >	< Last >
[arachNIDS] [local] [snort] ICMP L3retriever Ping	attempted-recon	46(7%)	1	20	21	2006-03-18 16:24:32	2006-05-04 09:16:4

ภาพ 89 แสดงเหตุการณ์ของการแจ้งเตือนภัยโปโตคอล ICMP "ICMP L3retriever Ping"

เป็นข้อความแจ้งเตือนภัยของ [7]ICMP echo request จากเครื่องที่ใช้ L3 "Retriever 1.5" ในการสแกน

ถือเป็นการแจ้งเตือนภัยที่เป็นแบบ True Positive

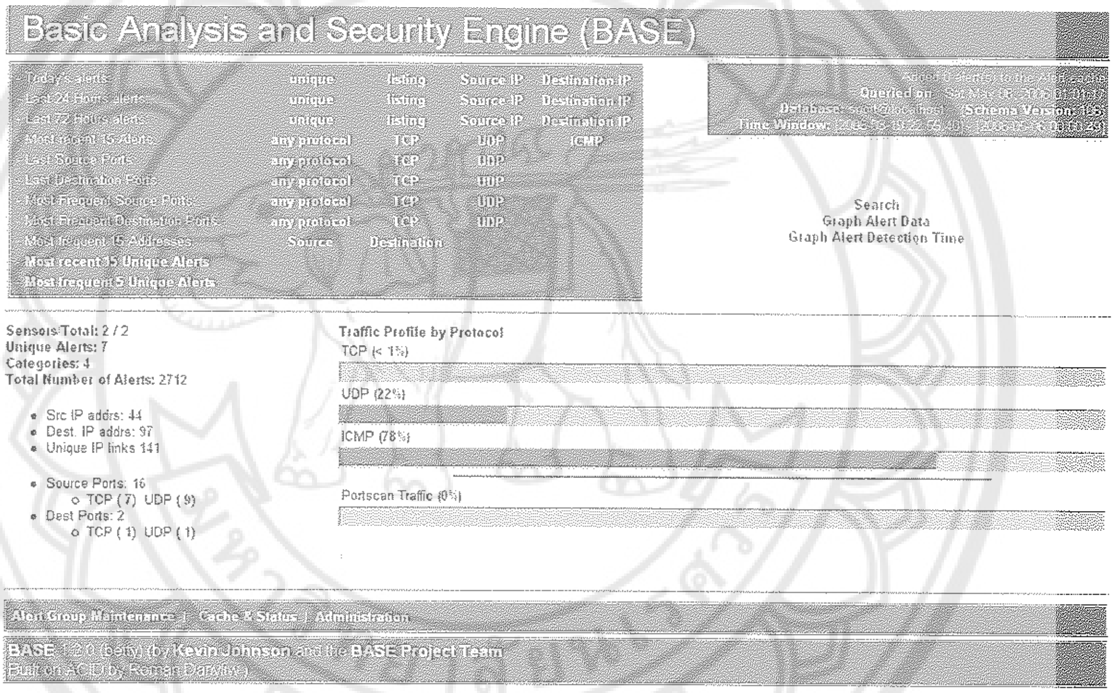
---

[7] http://www.snort.org/pub-bin/sigs.cgi?sid=466

4. **ภาควิชาฟิสิกส์**

การตรวจจับออกเป็นสัดส่วนได้ดังต่อไปนี้

- โปโตคอล TCP มีการแจ้งเตือนภัย 0 %
- โปโตคอล UDP มีการแจ้งเตือนภัย 4 %
- โปโตคอล ICMP มีการแจ้งเตือนภัย 96 %
- Portscan Traffic มีการแจ้งเตือนภัย 0 %



ภาพ 90 หน้าต่างหลักภาคฟิสิกส์แสดงการตรวจจับแพ็กเก็ต

4.1 โปโตคอล TCP มีการแจ้งเตือนภัย 1 % เป็นจำนวนทั้งสิ้น 7 ครั้ง

Displaying alerts 1-7 of 7 total

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#0-(2-1454)	[cve] [icat] [bugtraq] [arachNIDS] [local] [snort] WEB-IIS view source via translate header	2006-04-24 09:53:12	10.177.32.72:1513	10.177.96.5:80	TCP
#1-(2-818)	[cve] [icat] [bugtraq] [arachNIDS] [local] [snort] WEB-IIS view source via translate header	2006-04-13 02:03:45	10.177.32.70:1189	10.177.96.5:80	TCP
#2-(2-506)	[cve] [icat] [bugtraq] [arachNIDS] [local] [snort] WEB-IIS view source via translate header	2006-04-09 01:25:53	10.177.96.19:2997	10.177.96.5:80	TCP
#3-(2-247)	[cve] [icat] [bugtraq] [arachNIDS] [local] [snort] WEB-IIS view source via translate header	2006-04-05 21:23:09	10.210.8.117:4167	10.177.96.5:80	TCP
#4-(2-246)	[cve] [icat] [bugtraq] [arachNIDS] [local] [snort] WEB-IIS view source via translate header	2006-04-05 21:23:04	10.210.8.117:4165	10.177.96.5:80	TCP
#5-(2-245)	[cve] [icat] [bugtraq] [arachNIDS] [local] [snort] WEB-IIS view source via translate header	2006-04-05 21:23:03	10.210.8.117:4164	10.177.96.5:80	TCP
#6-(1-59)	[cve] [icat] [bugtraq] [arachNIDS] [local] [snort] WEB-IIS view source via translate header	2006-03-22 00:58:02	10.170.96.4:3640	10.170.96.5:80	TCP

ภาพ 91 โปโตคอล TCP มีการแจ้งเตือนภัย 1 % เป็นจำนวนทั้งสิ้น 7 ครั้ง

คำอธิบาย

เป็นการแจ้งเตือนภัยที่มีข้อความแจ้งว่า "WEB-IIS view source via translate header" ช่องโหว่ของ Web Server และ Services ที่ใช้งาน โดยปกติมักติดตั้ง Web Server หรือ HTTP Server ในแบบ Default คือไม่ได้แก้ไขค่าเริ่มต้นต่างๆ ที่มากับตัว Web Server ทำให้เกิดช่องโหว่ที่แฮกเกอร์สามารถนำมาใช้ได้ ระบบอาจเกิดปัญหาเช่น ปัญหา DoS Attack ทำให้ Web Server ไม่สามารถทำงานได้ หรือปัญหาการถูกโจมตีจนแฮกเกอร์สามารถ "ยึด" หรือ "Compromised" เครื่อง Web Server นั้นได้ และ สามารถเปลี่ยนหน้าเว็บเพ็จ ตลอดจนสามารถก๊อบปี้ไฟล์ข้อมูลได้
ช่องโหว่มักเกิดขึ้นเป็นประจำกับ Web Server IIS ของ Microsoft Windows NT/2000 ปกติเป็นเวอร์ชัน 3.0, 4.0 และ 5.0 ตามลำดับ สำหรับเวอร์ชัน 6.0 ที่มากับ Windows Server 2003 มีการปิดกั้นช่องโหว่ต่างๆ มาอย่างดีเมื่อเทียบกับเวอร์ชันก่อนหน้านี้ สำหรับ Apache Web Server ที่ทำงานบน Microsoft Windows ก็มีช่องโหว่เช่นกัน

วิธีการแก้ปัญหา

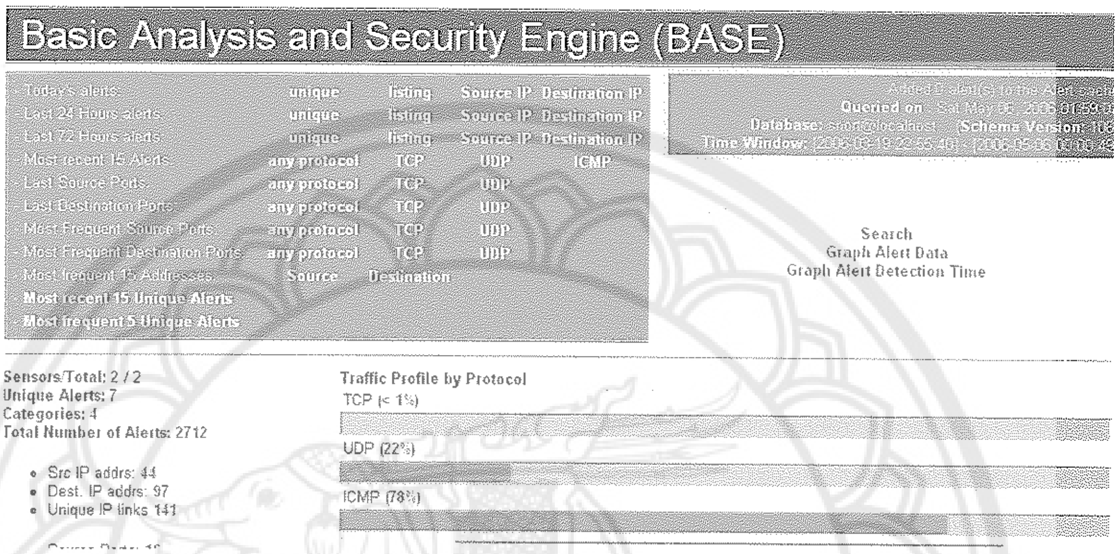
การลง "Patch" "Hotfix" หรือ อัพเดท Services Pack ล่าสุดของไมโครซอฟท์ เป็นทางออกที่ดีที่สุดในการป้องกันปัญหานี้ การติดตั้ง "Host-based IDS/IPS" ก็เป็นทางออกอีกทางหนึ่ง นอกจากนี้การติดตั้ง "Network-based IDS/IPS" ในลักษณะ In-line ก็สามารถช่วยได้ การเปลี่ยนแปลงค่า Default ต่างๆ หลังการติดตั้งก็เป็นเรื่องที่ต้องทำเช่นกัน รวมถึงการเก็บ Log File ในลักษณะ Remote Log โดยส่ง Log ไปเก็บที่ "Centralized Log Server" ก็เป็นแนวคิดที่ดีเพื่อเราสามารถจะตรวจสอบได้ภายหลังจากการโจมตีโดยไวรัสหรือแฮกเกอร์ การเปลี่ยนจาก IIS 5.0 มาใช้ IIS 6.0 ก็เป็นแนวทางที่ดี แต่ต้องดูเรื่อง "Compatibility" ของ Web Application ด้วย

สามารถอ่านและวิธีการป้องกันเพิ่มเติมได้ที่

http://www.microsoft.com/technet/security/bulletin/MS00-058.mspx

ถือเป็นการแจ้งเตือนภัยที่เป็นแบบ True Positive

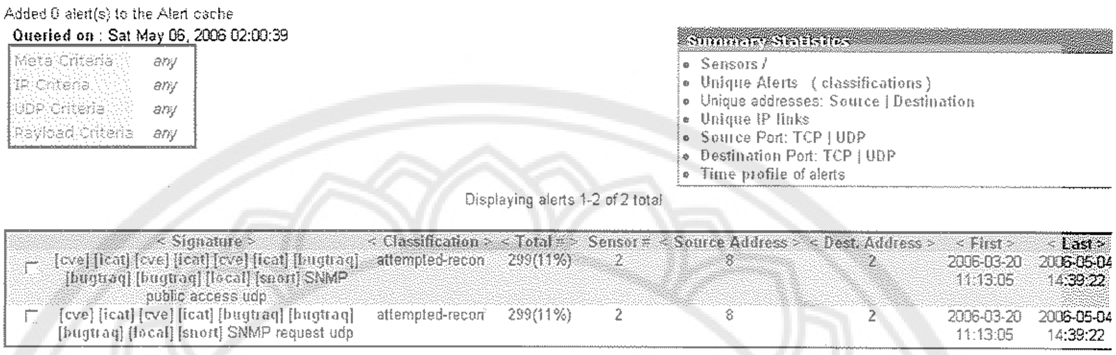
4.2 โปโตคอล UDP มีการแจ้งเตือนภัย 22 %



ภาพ 92 โปโตคอล UDP มีการแจ้งเตือนภัย 22 %

ภาพ 93 โปโตคอล UDP มีการแจ้งเตือนภัย 22 % เป็นจำนวนทั้งสิ้น 598 ครั้ง

แบ่งแยกตามเหตุการณ์ที่สามารถตรวจจับการบุกรุกได้ ดังต่อไปนี้



< Signature >	< Classification >	< Total # >	Sensor #	< Source Address >	< Dest. Address >	< First >	< Last >
[cve] [icat] [cve] [icat] [cve] [icat] [bugtraq] [bugtraq] [bugtraq] [local] [snort] SNMP public access udp	attempted-recon	299(11%)	2	8	2	2006-03-20 11:13:05	2006-05-04 14:39:22
[cve] [icat] [cve] [icat] [bugtraq] [bugtraq] [bugtraq] [local] [snort] SNMP request udp	attempted-recon	299(11%)	2	8	2	2006-03-20 11:13:05	2006-05-04 14:39:22

ภาพ 94 แสดงการแจ้งเตือนภัยโปรโตคอล UDP แบ่งแยกตามเหตุการณ์(Unique Alerts)

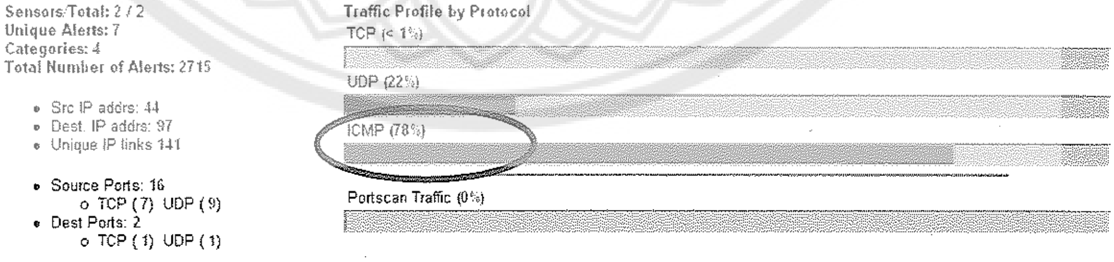
เป็นเหตุการณ์การแจ้งเตือนภัยเกี่ยวกับ **ช่วงโหว่ SNMP Service** จากการโดน Port scanning เป็นเหตุการณ์ที่ใช้ร้องขอติดต่อผ่านโปโตคอล SNMP ด้วย port 161

คำอธิบาย

เป็นช่วงโหว่ SNMP Service สามารถย้อนไปอ่านรายละเอียดได้ที่ในหน้าที่ 10-5

ถือเป็นการแจ้งเตือนภัยที่เป็นแบบ True Positive

4.3 โปโตคอล ICMP มีการแจ้งเตือนภัย 78 %



ภาพ 95 แสดงการแจ้งเตือนภัยโปโตคอล ICMP มีการแจ้งเตือนภัย 78 %

เป็นจำนวนทั้งสิ้น 2095 ครั้ง

Displaying alerts 1-50 of 2095 total

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto
#0-(2-2656)	[local] [snort] ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	2006-05-06 02:49:38	10.177.96.5	10.210.8.117	ICMP
#1-(2-2655)	[local] [snort] ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	2006-05-06 02:49:36	10.177.96.5	10.210.8.117	ICMP
#2-(2-2654)	[local] [snort] ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	2006-05-06 02:49:35	10.177.96.5	10.210.8.117	ICMP
#3-(2-2653)	[local] [snort] ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	2006-05-06 00:00:49	10.177.96.5	10.177.32.108	ICMP
#4-(2-2652)	[local] [snort] ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	2006-05-06 00:00:48	10.177.96.5	10.177.32.108	ICMP

ภาพ 96 แสดงการแจ้งเตือนภัยโปโตคอล ICMP เป็นจำนวนทั้งสิ้น 2095 ครั้ง

แบ่งแยกตามเหตุการณ์ที่สามารถตรวจจับการบุกรุกได้ ดังต่อไปนี้

Displaying alerts 1-3 of 3 total

< Signature >	< Classification >	< Total # >	Sensor #	< Source Address >	< Dest. Address >	< First >	< Last >
[arachNIDS] [local] [snort] ICMP L3retriever Ping	attempted-recon	63(2%)	2	26	22	2006-03-19 22:55:40	2006-05-02 13:08:23
[local] [snort] ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	misc-activity	1979(73%)	2	2	73	2006-03-22 00:52:55	2006-05-06 02:49:38
[arachNIDS] [local] [snort] ICMP PING NMAP	attempted-recon	53(2%)	1	4	1	2006-04-03 09:29:04	2006-05-04 10:31:48

ภาพ 97 แสดงการแจ้งเตือนภัยโปโตคอล ICMP แบ่งแยกตามเหตุการณ์ที่สามารถตรวจจับการบุก

รุก (Unique Alerts)

ซึ่งแบ่งออกได้ 3 เหตุการณ์

4.3.1 เหตุการณ์ที่ 1เหตุการณ์ "ICMP L3retriever Ping" จำนวนทั้งสิ้น 63 ครั้ง

Displaying alerts 1-1 of 1 total

< Signature >	< Classification >	< Total # >	Sensor #	< Source Address >	< Dest. Address >	< First >	< Last >
[arachNIDS] [local] [snort] ICMP L3retriever Ping	attempted-recon	63(2%)	2	26	22	2006-03-19 22:55:40	2006-05-02 13:08:23

ภาพ 98 แสดงเหตุการณ์ของการแจ้งเตือนภัยโปโตคอล ICMP "ICMP L3retriever Ping"

เป็นข้อความแจ้งเตือนภัยของ [8]ICMP echo request จากเครื่องที่ใช้ L3 "Retriever 1.5" ในการสแกน

ถือเป็นการแจ้งเตือนภัยที่เป็นแบบ True Positive

[8] http://www.snort.org/pub-bin/sigs.cgi?sid=466

4.3.2 เหตุการณ์ "ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited " จำนวนทั้งสิ้น 1979 ครั้ง

	< Signature >	< Classification >	< Total # >	Sensor #	< Source Address >	< Dest. Address >	< First >	< Last >
☐	[local] [snort] ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	misc-activity	1979(73%)	2	2	73	2006-03-22 00:52:55	2006-05-06 02:49:38

ภาพ 99 แสดงเหตุการณ์ของการแจ้งเตือนภัยโปโตคอล ICMP "ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited "

คำอธิบาย

ICMP ชนิดไม่สามารถติดต่อสถานีปลายทาง

เป็นการแจ้งเตือนภัยเกี่ยวกับการป้องกันการโจมตีที่เกิดขึ้นแบบ Denial of Service สามารถย้อนไปอ่านรายละเอียดได้ที่ในหน้าที่ 10-25

ถือเป็นการแจ้งเตือนภัยที่เป็นแบบ True Positive

4.3.3 เหตุการณ์ "ICMP PING NMAP" จำนวนทั้งสิ้น 53 ครั้ง

Displaying alerts 1-1 of 1 total

	< Signature >	< Classification >	< Total # >	Sensor #	< Source Address >	< Dest. Address >	< First >	< Last >
☐	[arachNIDS] [local] [snort] ICMP PING NMAP	attempted-recon	53(2%)	1	4	1	2006-04-03 09:29:04	2006-05-04 10:31:48

ภาพ 100 แสดงเหตุการณ์ของการแจ้งเตือนภัยโปโตคอล ICMP "ICMP PING NMAP"

เหตุการณ์ "ICMP PING NMAP" เป็นเหตุการณ์ที่สามารถอธิบายได้ดังข้อความข้างล่างต่อไปนี้ เป็นการแจ้งเตือนภัยจากการโดน Port scanning ด้วยโปรแกรม NMAP

Displaying alerts 1-4 of 4 total

Source FQDN	< Source IP >	Direction	< Destination IP >	Destination FQDN	Protocol	Unique Dst Ports	Unique Events	Total Event
Unable to resolve address	10.177.64.105	-->	10.177.96.5	*Unable to resolve address*	ICMP	0	1	44
Unable to resolve address	10.177.64.33	-->	10.177.96.5	*Unable to resolve address*	ICMP	0	1	2
Unable to resolve address	10.177.80.4	-->	10.177.96.5	*Unable to resolve address*	ICMP	0	1	1
Unable to resolve address	10.177.64.56	-->	10.177.96.5	*Unable to resolve address*	ICMP	0	1	6

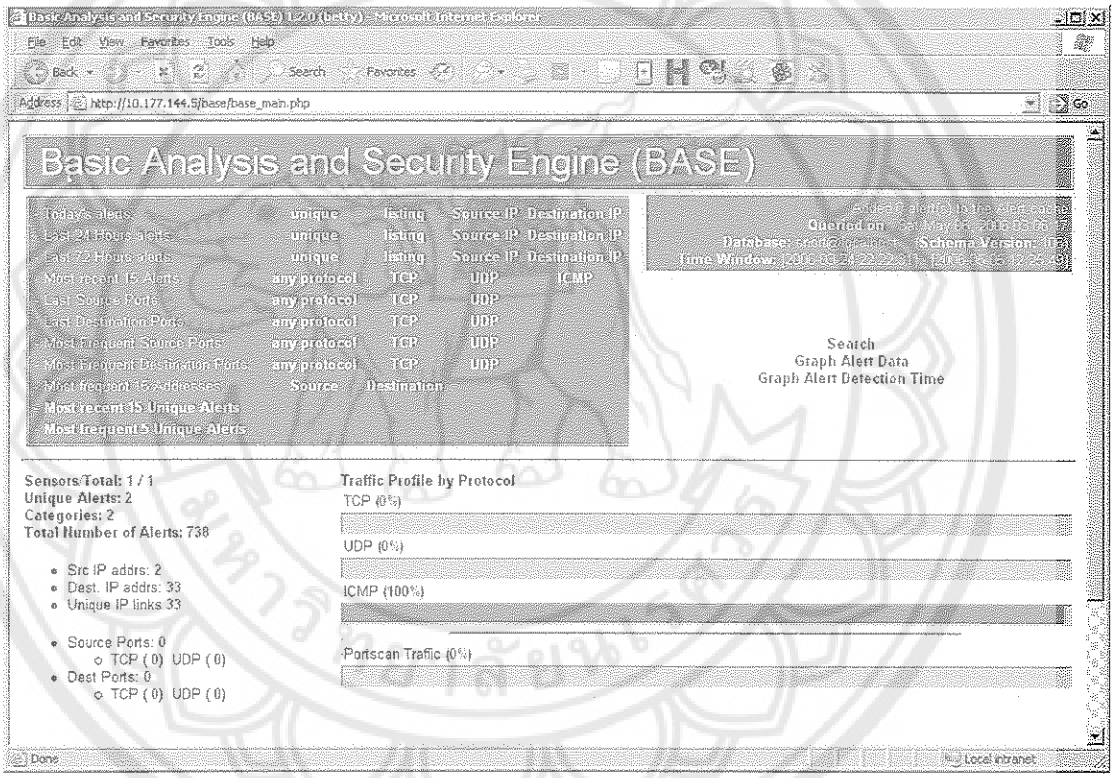
ภาพ 101 แสดงเหตุการณ์ของการแจ้งเตือนภัยโปโตคอล ICMP "ICMP PING NMAP" ตามหมายเลขไอพีต้นทางไปยังหมายเลขไอพีปลายทาง

ถือเป็นการแจ้งเตือนภัยที่เป็นแบบ True Positive

5. **ภาควิชาสถิติ**

การแบ่งค่าของการตรวจจับออกได้ดังต่อไปนี้

- โปโตคอล TCP มีการแจ้งเตือนภัย 0 %
- โปโตคอล UDP มีการแจ้งเตือนภัย 0 %
- โปโตคอล ICMP มีการแจ้งเตือนภัย 100 %
- Portscan Traffic มีการแจ้งเตือนภัย 0 %



ภาพ 102 หน้าต่างหลักภาควิชาสถิติแสดงการตรวจจับแพ็กเก็ต

5.1 โปรโตคอล ICMP มีการแจ้งเตือนภัย 100 %

Sensors/Total: 1 / 1
Unique Alerts: 2
Categories: 2
Total Number of Alerts: 738

- Src IP addrs: 2
- Dest. IP addrs: 33
- Unique IP links 33

- Source Ports: 0
  - TCP (0) UDP (0)
- Dest Ports: 0
  - TCP (0) UDP (0)

Traffic Profile by Protocol
TCP (0%)
UDP (0%)
ICMP (100%)
Portscan Traffic (0%)

ภาพ 103 แสดงการแจ้งเตือนภัยโปรโตคอล ICMP จำนวน 100 %

เป็นจำนวนทั้งสิ้น 738 ครั้ง

Displaying alerts 1-50 of 738 total

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Prot
#0-(1-738)	[local] [snort] ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	2006-05-05 12:25:49	10.177.144.5	10.177.64.33	ICMP
#1-(1-737)	[local] [snort] ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	2006-05-05 12:25:46	10.177.144.5	10.177.64.33	ICMP
#2-(1-736)	[local] [snort] ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	2006-05-05 12:10:07	10.177.144.5	10.177.64.33	ICMP
#3-(1-735)	[local] [snort] ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	2006-05-05 12:10:05	10.177.144.5	10.177.64.33	ICMP

ภาพ 104 แสดงการแจ้งเตือนภัยโปรโตคอล ICMP เป็นจำนวนทั้งสิ้น 738 ครั้ง

แบ่งแยกตามเหตุการณ์ที่สามารถตรวจจับการบุกรุกได้ ดังต่อไปนี้

Displaying alerts 1-2 of 2 total

< Signature >	< Classification >	< Total # >	Sensor #	< Source Address >	< Dest. Address >	< First >	< Last >
[local] [snort] ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	misc-activity	737(100%)	1	1	32	2006-03-24 22:22:31	2006-05-05 12:25:49
[arachNIDS] [local] [snort] ICMP PING NMAP	attempted-recon	1(0%)	1	1	1	2006-05-02 17:56:22	2006-05-02 17:56:22

ภาพ 105 แบ่งแยกตามเหตุการณ์ที่สามารถตรวจจับการบุกรุกได้ (Unique Alerts)

ซึ่งแบ่งออกได้ 2 เหตุการณ์

5.1.1 เหตุการณ์ "ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited " จำนวนทั้งสิ้น 737 ครั้ง

< Signature >	< Classification >	< Total # >	Sensor #	< Source Address >	< Dest. Address >	< First >	< Last >
[local] [snort] ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	misc-activity	737(100%)	1	1	32	2006-03-24 22:22:31	2006-05-05 12:25:49

รูป 106 แสดงเหตุการณ์ของการแจ้งเตือนภัยโปโตคอล ICMP "ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited"

คำอธิบาย

ICMP ชนิดไม่สามารถติดต่อสถานีปลายทาง

เป็นการแจ้งเตือนภัยเกี่ยวกับการป้องกันการโจมตีที่เกิดขึ้นแบบ Denial of Service สามารถย้อนไปอ่านรายละเอียดได้ที่ในหน้าที่ 10-25

ถือเป็นการแจ้งเตือนภัยที่เป็นแบบ True Positive

5.1.2 เหตุการณ์ "ICMP PING NMAP" จำนวนทั้งสิ้น 1 ครั้ง

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#0-(1-669)	[arachNIDS] [local] [snort] ICMP PING NMAP	2006-05-02 17:56:22	10.177.64.33	10.177.144.5	ICMP

ภาพ 107 แสดงเหตุการณ์ของการแจ้งเตือนภัยโปโตคอล ICMP "ICMP PING NMAP"

เหตุการณ์ "ICMP PING NMAP" เป็นเหตุการณ์ที่สามารถอธิบายได้ดังข้อความข้างล่างต่อไปนี้ เป็นการแจ้งเตือนภัยจากการโดน Port scanning ด้วยโปรแกรม NMAP

Source FQDN	< Source IP >	Direction	< Destination IP >	Destination FQDN	Protocol	Unique Dst Ports	Unique Events	Total Events
Unable to resolve address	10.177.64.33	-->	10.177.144.5	*Unable to resolve address*	ICMP	0	1	1

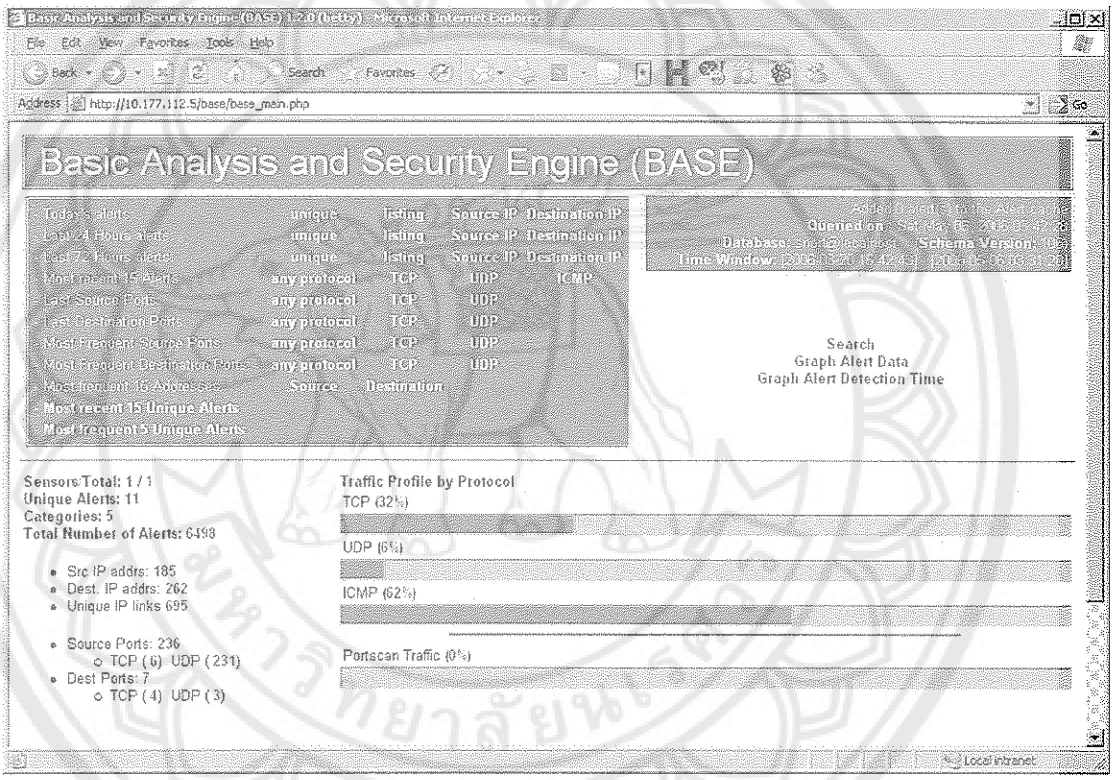
ภาพ 108 แสดงเหตุการณ์ของการแจ้งเตือนภัยโปโตคอล ICMP "ICMP PING NMAP" ตามหมายเลขไอพีต้นทางไปยังหมายเลขไอพีปลายทาง

ถือเป็นการแจ้งเตือนภัยที่เป็นแบบ True Positive

6. ภาควิชาวิทยาการคอมพิวเตอร์

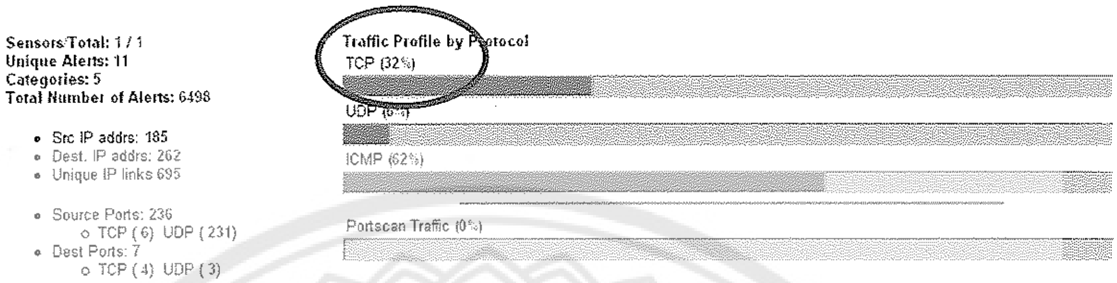
การแบ่งค่าของการตรวจจับออกได้ดังต่อไปนี้

- โปโตคอล TCP มีการแจ้งเตือนภัย 32%
- โปโตคอล UDP มีการแจ้งเตือนภัย 6 %
- โปโตคอล ICMP มีการแจ้งเตือนภัย 62 %
- Portscan Traffic มีการแจ้งเตือนภัย 0 %



ภาพ 109 หน้าต่างหลักภาควิชาวิทยาการคอมพิวเตอร์แสดงการตรวจจับแพ็กเก็ต

6.1 โปรโตคอล TCP มีการแจ้งเตือนภัย 32%



ภาพ 110 โปรโตคอล TCP มีการแจ้งเตือนภัย 32%

เป็นจำนวนทั้งสิ้น 2070 ครั้ง

Displaying alerts 1-50 of 2070 total

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Pro
#0-(1-5804)	[cve] [icat] [bugtraq] [arachNIDS] [local] [snort] WEB-IIS view source via translate header	2006-04-28 14:44:44	10.177.112.73:1754	10.177.112.5:80	TCP
#1-(1-5447)	[cve] [icat] [bugtraq] [arachNIDS] [local] [snort] WEB-IIS view source via translate header	2006-04-26 15:24:55	10.177.96.119:2182	10.177.112.5:80	TCP
#2-(1-4296)	[snort] (snort_decoder): Experimental Tcp Options found	2006-04-10 15:29:14	10.177.112.88:1024	88.152.64.100:76	TCP

ภาพ 111 แสดงการแจ้งเตือนภัยโปรโตคอล TCP เป็นจำนวนทั้งสิ้น 2070 ครั้ง

แบ่งแยกตามเหตุการณ์ที่สามารถตรวจจับการบุกรุกได้ ดังต่อไปนี้

Displaying alerts 1-3 of 3 total

< Signature >	< Classification >	< Total # >	Sensor #	< Source Address >	< Dest. Address >	< First >	< Last >
[cve] [icat] [bugtraq] [arachNIDS] [local] [snort] WEB-IIS view source via translate header	web-application-activity	4(0%)	1	4	1	2006-03-22 00:21:43	2006-04-28 14:44:44
[local] [snort] ATTACK-RESPONSES 403 Forbidden	attempted-recon	2(0%)	1	1	1	2006-03-23 01:34:17	2006-04-05 14:33:53
[snort] (snort_decoder): Experimental Tcp Options found	*unclassified*	2064(32%)	1	1	4	2006-04-10 10:52:47	2006-04-10 15:29:14

ภาพ 112 แบ่งแยกตามเหตุการณ์ที่สามารถตรวจจับการบุกรุกได้ (Unique Alerts)

ซึ่งแบ่งออกได้ 3 เหตุการณ์

6.1.1 เหตุการณ์ที่ 1 "WEB-IIS view source via translate header" จำนวน 4 ครั้ง

< Signature >	< Classification >	< Total # >	Sensor #	< Source Address >	< Dest. Address >	< First >	< Last >
[cve] [icat] [bugtraq] [arachNIDS] [local] [snort] WEB-IIS view source via translate header	web-application-activity	4(0%)	1	4	1	2006-03-22 00:21:43	2006-04-28 14:44:44

ภาพ 113 เหตุการณ์ที่ 1 "WEB-IIS view source via translate header"

คำอธิบาย

เป็นการแจ้งเตือนภัยที่มีข้อความแจ้งว่า "WEB-IIS view source via translate header" ช่องโหว่ของ Web Server และ Services ที่ใช้งาน โดยปกติมักติดตั้ง Web Server หรือ HTTP Server ในแบบ Default คือไม่ได้แก้ไขค่าเริ่มต้นต่างๆ ที่มากับตัว Web Server ทำให้เกิดช่องโหว่ที่แฮกเกอร์สามารถนำมาใช้ได้ ระบบอาจเกิดปัญหาเช่น ปัญหา DoS Attack ทำให้ Web Server ไม่สามารถทำงานได้ หรือปัญหาการถูกโจมตีจนแฮกเกอร์สามารถ "ยึด" หรือ "Compromised" เครื่อง Web Server นั้นได้ และ สามารถเปลี่ยนหน้าเว็บเพ็จ ตลอดจนสามารถก๊อบปี้ไฟล์ข้อมูลได้

ช่องโหว่มักเกิดขึ้นเป็นประจำกับ Web Server IIS ของ Microsoft Windows NT/2000 ปกติเป็นเวอร์ชัน 3.0, 4.0 และ 5.0 ตามลำดับ สำหรับเวอร์ชัน 6.0 ที่มากับ Windows Server 2003 มีการปิดกั้นช่องโหว่ต่างๆ มาอย่างดีเมื่อเทียบกับเวอร์ชันก่อนหน้านี้ สำหรับ Apache Web Server ที่ทำงานบน Microsoft Windows ก็มีช่องโหว่เช่นกัน

วิธีการแก้ปัญหา

การลง "Patch" "Hotfix" หรือ อัพเดท Services Pack ล่าสุดของไมโครซอฟท์ เป็นทางออกที่ดีที่สุดในการป้องกันปัญหานี้ การติดตั้ง "Host-based IDS/IPS" ก็เป็นทางออกอีกทางหนึ่ง นอกจากนี้การติดตั้ง "Network-based IDS/IPS" ในลักษณะ In-line ก็สามารถช่วยได้ การเปลี่ยนแปลงค่า Default ต่างๆ หลังการติดตั้งก็เป็นเรื่องที่ต้องทำเช่นกัน รวมถึงการเก็บ Log File ในลักษณะ Remote Log โดยส่ง Log ไปเก็บที่ "Centralized Log Server" ก็เป็นแนวคิดที่ดีเพื่อเราสามารถจะตรวจสอบได้ภายหลังจากการโจมตีโดยไวรัสหรือแฮกเกอร์ การเปลี่ยนจาก IIS 5.0 มาใช้ IIS 6.0 ก็เป็นแนวทางที่ดี แต่ต้องดูเรื่อง "Compatibility" ของ Web Application ด้วย

สามารถอ่านและวิธีการป้องกันเพิ่มเติมได้ที่

http://www.microsoft.com/technet/security/bulletin/MS00-058.mspx

ถือเป็นการแจ้งเตือนภัยที่เป็นแบบ True Positive

6.1.2 เหตุการณ์ที่ 2 “ATTACK-RESPONSES 403 Forbidden” จำนวน 2 ครั้ง

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#0-(1-333)	[local] [snort] ATTACK-RESPONSES 403 Forbidden	2006-03-23 01:34:17	10.177.112.5:80	10.177.160.39:3511	TCP
#1-(1-1774)	[local] [snort] ATTACK-RESPONSES 403 Forbidden	2006-04-05 14:33:53	10.177.112.5:80	10.177.160.39:2567	TCP

ภาพ 114 เหตุการณ์ “ATTACK-RESPONSES 403 Forbidden” จำนวน 2 ครั้ง

คำอธิบาย

*[9]Error 403 นั้นเป็นความผิดพลาดจากการที่ผู้ใช้พยายามเข้าใช้งานส่วนใดๆ ของเว็บไซต์โดยไม่ได้รับอนุญาต” เป็นการแจ้งเตือนภัยที่มีการพยายามเข้ามาทางรู้รั่วของบริการเว็บเซิร์ฟเวอร์ที่ใช้งาน Apache

ถือเป็นการแจ้งเตือนภัยที่เป็นแบบ True Positive

6.1.3 เหตุการณ์ที่ 3 “(snort_decoder): Experimental Tcp Options found” จำนวน 2064 ครั้ง

< Signature >	< Classification >	< Total # >	Sensor #	< Source Address >	< Dest. Address >	< First >	< Last >
[snort] (snort_decoder): Experimental Tcp Options found	*unclassified*	2064(32%)	1	1	4	2006-04-10 10:52:47	2006-04-10 15:29:14

ภาพ 115 เหตุการณ์ที่ 3 “(snort_decoder): Experimental Tcp Options found”

คำอธิบาย

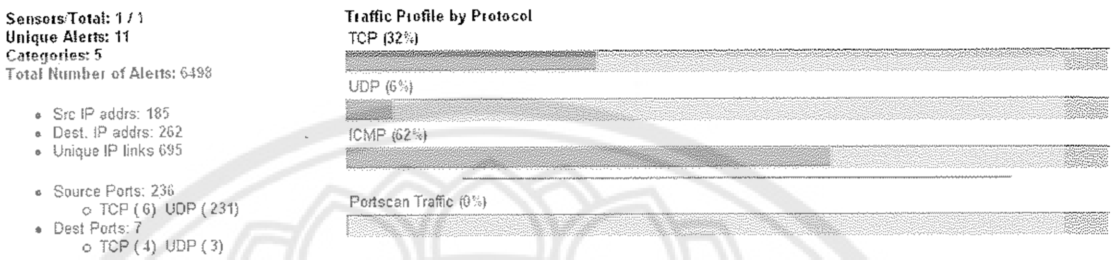
เป็นเหตุการณ์ที่สามารถอ้างอิงได้จากกฎของ Snort เอง แต่เมื่อได้ไปตรวจสอบหายเลขไอพีที่สามารถตรวจจับการบุกรุกได้พบว่าเป็นการใช้งาน Application ที่เกี่ยวกับใช้งานแบบ Bit Torrent

ถือเป็นการแจ้งเตือนภัยที่เป็นแบบ True Positive **เพียงแต่ยังไม่สามารถตรวจจับลงลึกแสดงว่าเป็นการใช้งานบริการแบบ** Bit Torrent

---

9 มนัชยา ชมธวัช, Apache Security Checklist, http://thaicert.nectec.or.th/paper/unix_linux/apache_chklist.php#8

6.2 โปรโตคอล UDP มีการแจ้งเตือนภัย 6%



ภาพ 116 แสดง โปรโตคอล UDP มีการแจ้งเตือนภัย 6%

เป็นจำนวนทั้งสิ้น 418 ครั้ง

Displaying alerts 1-50 of 418 total

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#0-(1-6489)	[nessus] [local] [snort] MS-SQL ping attempt	2006-05-05 20:15:42	10.177.112.78:1079	255.255.255.255:1434	UDP
#1-(1-6464)	[nessus] [local] [snort] MS-SQL ping attempt	2006-05-04 14:47:27	10.177.112.17:1046	255.255.255.255:1434	UDP
#2-(1-6452)	[nessus] [local] [snort] MS-SQL ping attempt	2006-05-04 10:55:54	10.177.112.17:1046	255.255.255.255:1434	UDP
#3-(1-6428)	[nessus] [local] [snort] MS-SQL ping attempt	2006-05-04 08:45:34	10.177.112.17:1045	255.255.255.255:1434	UDP

ภาพ 117 แสดงการแจ้งเตือนภัยโปรโตคอล UDP เป็นจำนวนทั้งสิ้น 418 ครั้ง

แบ่งแยกตามเหตุการณ์ที่สามารถตรวจจับการบุกรุกได้ ดังต่อไปนี้

Displaying alerts 1-5 of 5 total

< Signature >	< Classification >	< Total # >	Sensor #	< Source Address >	< Dest. Address >	< First >	< Last >
[nessus] [local] [snort] MS-SQL ping attempt	misc-activity	316(5%)	1	77	1	2006-03-21 09:09:01	2006-05-05 20:15:42
[local] [snort] SCAN UPnP service discover attempt	network-scan	15(0%)	1	3	1	2006-03-22 09:31:41	2006-03-30 11:07:58
[cve] [icat] [cve] [icat] [cve] [icat] [bugtraq] [bugtraq] [bugtraq] [local] [snort] SNMP public access udp	attempted-recon	34(1%)	1	9	2	2006-03-22 14:02:36	2006-05-01 17:37:04
[cve] [icat] [cve] [icat] [bugtraq] [bugtraq] [bugtraq] [local] [snort] SNMP request udp	attempted-recon	36(1%)	1	9	2	2006-03-22 14:02:36	2006-05-01 17:37:04
[cve] [icat] [cve] [icat] [bugtraq] [bugtraq] [bugtraq] [local] [snort] SNMP Broadcast request	attempted-recon	17(0%)	1	5	1	2006-03-23 15:43:07	2006-04-01 19:19:03

ภาพ 118 แบ่งแยกตามเหตุการณ์ที่สามารถตรวจจับการบุกรุก (Unique Alerts)

สามารถแบ่งออกได้ 5 เหตุการณ์ดังต่อไปนี้

6.2.1 เหตุการณ์ที่ 1 “MS-SQL ping attempt” เป็นจำนวนทั้งสิ้น 316 ครั้ง

< Signature >	< Classification >	< Total # >	Sensor #	< Source Address >	< Dest. Address >	< First >	< Last >
[nessus] [local] [snort] MS-SQL ping attempt	misc-activity	316(5%)	1	77	1	2006-03-21 09:09:01	2006-05-05 20:15:42

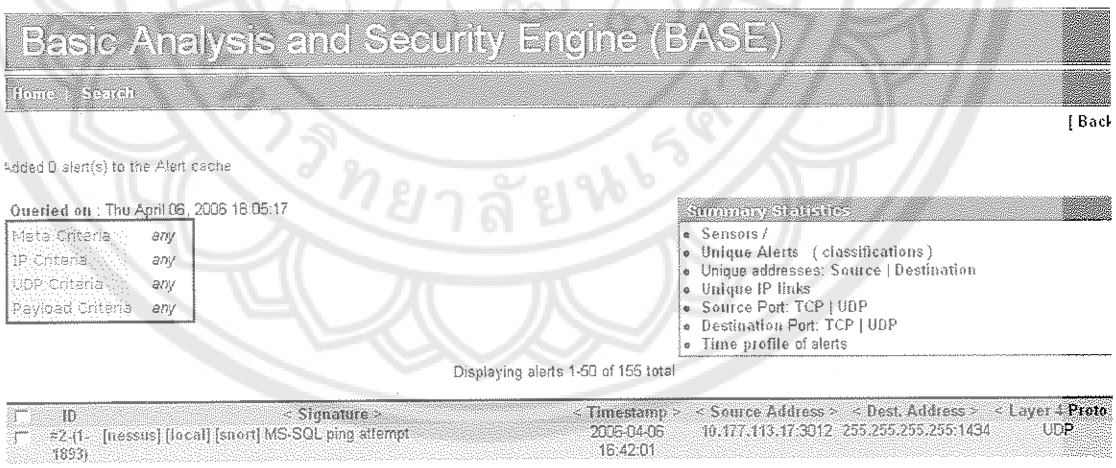
ภาพ 119 แสดง “MS-SQL ping attempt” เป็นจำนวนทั้งสิ้น 316 ครั้ง

คำอธิบาย

MS-SQL ping attempt เป็นช่องโหว่สำคัญของระบบปฏิบัติการ Windows นั้นคือ W3 Microsoft SQL Server สามารถย้อนไปอ่านรายละเอียดได้ที่ในหน้าที่ 10-19

ถือเป็นการแจ้งเตือนภัยที่เป็นแบบ True Positive

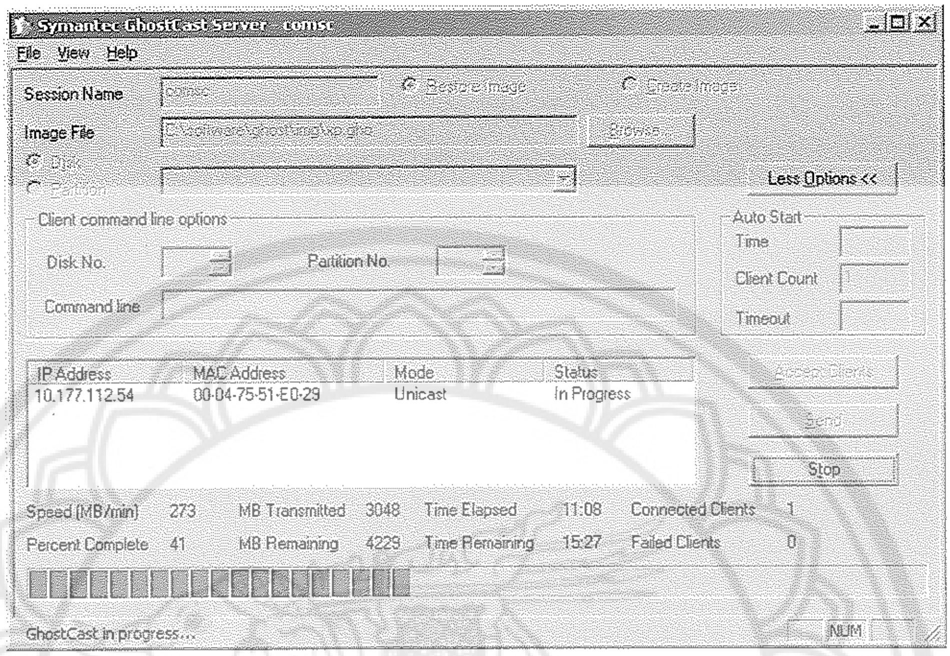
เหตุการณ์ที่ตรวจสอบได้อย่างหนึ่งของ MS-SQL ping attempt มีการแจ้งเตือนภัยพบว่า ได้ทำการ copy Hard disk โดยผ่านโปรแกรม Ghost ในระบบเครือข่ายคอมพิวเตอร์ของภาควิชาวิทยาการคอมพิวเตอร์



ภาพ 120 การแจ้งเตือนว่าในกรณีทำการ copy Hard disk โดยผ่านโปรแกรม Ghost ในระบบเครือข่ายคอมพิวเตอร์ ของภาควิชาวิทยาการคอมพิวเตอร์

ได้ทำการตรวจสอบกับทางเจ้าหน้าที่ดูแลของภาควิชา พบว่าหมายเลขไอพีทั้งต้นทางและปลายทางกำลังติดต่อเพื่อ copy ข้อมูลของ Harddisk

- หมายเลขไอพี 10.177.112.17 คือ File Server ให้ copy ไฟล์



ภาพ 121 โปรแกรม Ghost ขณะเปิดใช้บริการ

6.2.2 เหตุการณ์ที่ 2 "SCAN UPnP service discover attempt" เป็นจำนวนทั้งสิ้น 15 ครั้ง

< Signature >	< Classification >	< Total # >	Sensor #	< Source Address >	< Dest. Address >	< First >	< Last >
[local] [snort] SCAN UPnP service discover attempt	network-scan	15(0%)	1	3	1	2006-03-22 09:31:41	2006-03-30 11:07:58

ภาพ 122 แสดง "SCAN UPnP service discover attempt" เป็นจำนวนทั้งสิ้น 15 ครั้ง

คำอธิบาย

เป็นช่องโหว่ The Universal Plug and Play (UPnP) สามารถย้อนไปอ่านรายละเอียดได้ที่ในหน้าที่ 10-10

ถือเป็นการแจ้งเตือนภัยที่เป็นแบบ True Positive

6.2.3 เหตุการณ์ที่ 3 เป็นการแจ้งเตือนภัยที่มีข้อความแจ้งว่า "SNMP public access udp" ทั้งหมด 34 ครั้ง

6.2.4 เหตุการณ์ที่ 4 เป็นการแจ้งเตือนภัยที่มีข้อความแจ้งว่า "SNMP request udp" ทั้งหมด 36 ครั้ง

6.2.5 เหตุการณ์ที่ 5 เป็นการแจ้งเตือนภัยที่มีข้อความแจ้งว่า “SNMP Broadcast request” ทั้งหมด 17 ครั้ง

	[cve] [icat] [cve] [icat] [cve] [icat] [bugtraq] [bugtraq] [bugtraq] [local] [snort] SNMP public access udp	attempted-recon	34(1%)	1	9	2	2006-03-22 14:02:36	2006-05-01 17:37:04
	[cve] [icat] [cve] [icat] [bugtraq] [bugtraq] [bugtraq] [local] [snort] SNMP request udp	attempted-recon	36(1%)	1	9	2	2006-03-22 14:02:36	2006-05-01 17:37:04
	[cve] [icat] [cve] [icat] [bugtraq] [bugtraq] [bugtraq] [local] [snort] SNMP Broadcast request	attempted-recon	17(0%)	1	5	1	2006-03-23 15:43:07	2006-04-01 19:19:03

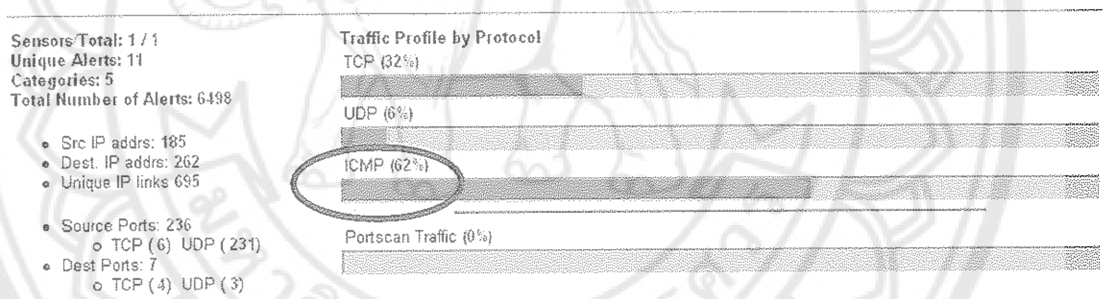
ภาพ 123 การแจ้งเตือนภัยเกี่ยวกับเป็นช่วงโหว่ SNMP Service

คำอธิบาย

เป็นช่วงโหว่ SNMP Service สามารถย้อนไปอ่านรายละเอียดได้ที่ในหน้าที่ 10-5

ถือเป็นการแจ้งเตือนภัยที่เป็นแบบ True Positives

6.3 โปโตคอล ICMP มีการแจ้งเตือนภัย 62 %



ภาพ 124 โปโตคอล ICMP มีการแจ้งเตือนภัย 62 %

เป็นจำนวนทั้งสิ้น 4010 ครั้ง

Displaying alerts 1-50 of 4010 total

	ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
	#0-(1-6498)	[local] [snort] ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	2006-05-06 03:31:20	10.177.112.5	10.210.8.63	ICMP
	#1-(1-6497)	[local] [snort] ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	2006-05-06 03:31:19	10.177.112.5	10.210.8.63	ICMP
	#2-(1-6496)	[local] [snort] ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	2006-05-06 03:31:17	10.177.112.5	10.210.8.63	ICMP

ภาพ 125 แสดงการแจ้งเตือนภัยโปรโตคอล ICMP เป็นจำนวนทั้งสิ้น 4010 ครั้ง

แบ่งแยกตามเหตุการณ์ที่สามารถตรวจจับการบุกรุกได้ ดังต่อไปนี้

Displaying alerts 1-3 of 3 total

< Signature >	< Classification >	< Total >	< Sensor >	< Source Address >	< Dest. Address >	< First >	< Last >
[local] [snort] ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	misc-activity	3311(51%)	1	1	108	2006-03-20 15:42:43	2006-05-06 03:31:20
[arachNIDS] [local] [snort] ICMP L3retriever Ping	attempted-recon	602(9%)	1	119	152	2006-03-20 16:19:48	2006-05-04 16:01:16
[arachNIDS] [local] [snort] ICMP PING NMAP	attempted-recon	97(1%)	1	7	2	2006-03-20 16:38:09	2006-05-04 10:34:05

ภาพ 126 แบ่งแยกตามเหตุการณ์ที่สามารถตรวจจับการบุกรุกได้ (Unique Alerts)

ซึ่งแบ่งออกได้ 3 เหตุการณ์

6.3.1 เหตุการณ์ "ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited " จำนวนทั้งสิ้น 3311 ครั้ง

Displaying alerts 1-1 of 1 total

< Signature >	< Classification >	< Total = >	Sensor #	< Source Address >	< Dest. Address >	< First >	< Last >
[local] [snort] ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	misc-activity	3311(51%)	1	1	108	2006-03-20 15:42:43	2006-05-06 03:31:20

ภาพ 127 แสดงเหตุการณ์ของการแจ้งเตือนภัยโปโตคอล ICMP "ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited "

"ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited " เป็นเหตุการณ์ที่สามารถอธิบายได้ดังข้อความข้างล่างต่อไปนี้

คำอธิบาย

ICMP ชนิดไม่สามารถติดต่อสถานีปลายทาง

เป็นการแจ้งเตือนภัยเกี่ยวกับการป้องกันการโจมตีที่เกิดขึ้นแบบ Denial of Service

ซึ่งหาก router ไม่สามารถส่ง datagram ไปยัง router หรือ host ถัดไปได้ router จะตอบกลับด้วย ICMP และใส่รหัสในฟิลด์ code เพื่อบอกสาเหตุของปัญหา

0 – 7	8 – 15	16 – 31
Type = 3	Code = 0 – 15	Checksum
ไม่ใช้งาน (มีค่าเป็น 0)		
Header IP + 64 bit แรกของข้อมูล		

ภาพ 128 ICMP datagram

Code	ความผิดพลาด	ความหมาย
0	Network unreachable	ไปไม่ถึงเครือข่าย
1	Host unreachable	ไปไม่ถึง host
2	Protocol unreachable	ไปไม่ถึง protocol ปลายทาง
3	Port unreachable	ไปไม่ถึง port
4	Fragmentation needed but the Do Not Fragment bit was set	จำเป็นต้องแบ่ง datagram แต่มีการกำหนดไม่ให้แบ่งแยก
5	Source route failed	เส้นทางที่กำหนดล้มเหลว
6	Destination network unknown	ไม่ปรากฏเครือข่ายปลายทาง
7	Destination host unknown	ไม่ปรากฏ host ปลายทาง
8	Source host isolated (obsolete)	
9	Destination network administratively prohibited	มีการป้องกันไม่ให้เข้าเครือข่ายปลายทาง
10	Destination host administratively prohibited	มีการป้องกันไม่ให้เข้า host ปลายทาง

ภาพ 129 Code ของ ICMP

ถือเป็นการแจ้งเตือนภัยที่เป็นแบบ True Positive

6.3.2 เหตุการณ์ที่ 2 "ICMP L3retriever Ping" จำนวนทั้งสิ้น 6.2 ครั้ง

Displaying alerts 1-1 of 1 total

	< Signature >	< Classification >	< Total # >	Sensor #	< Source Address >	< Dest. Address >	< First >	< Last >
☐	[arachNIDS] [local] [snort] ICMP L3retriever Ping	attempted-recon	602(9%)	1	119	152	2006-03-20 16:19:48	2006-05-04 16:01:16

ภาพ 130 แสดงเหตุการณ์ของการแจ้งเตือนภัยโปโตคอล ICMP "ICMP L3retriever Ping"

เป็นข้อความแจ้งเตือนภัยของ [10]ICMP echo request จากเครื่องที่ใช้ L3 "Retriever 1.5" ในการสแกน

ถือเป็นการแจ้งเตือนภัยที่เป็นแบบ True Positives

6.3.3 เหตุการณ์ที่ 3 "ICMP PING NMAP" จำนวนทั้งสิ้น 97 ครั้ง

Displaying alerts 1-1 of 1 total

< Signature >	< Classification >	< Total # >	Sensor #	< Source Address >	< Dest. Address >	< First >	< Last >
[arachNIDS] [local] [snort] ICMP PING NMAP	attempted-recon	97(1%)	1	7	2	2006-03-20 16:38:09	2006-05-04 10:34:05

ภาพ 131 แสดงเหตุการณ์ของการแจ้งเตือนภัยโปโตคอล ICMP "ICMP PING NMAP"

เหตุการณ์ "ICMP PING NMAP" เป็นเหตุการณ์ที่สามารถอธิบายได้ดังข้อความข้างล่างต่อไปนี้ เป็นการแจ้งเตือนภัยจากการโดน Port scanning ด้วยโปรแกรม NMAP

Displaying alerts 1-50 of 97 total

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#0-(1-5)	[arachNIDS] [local] [snort] ICMP PING NMAP	2006-03-20 16:38:09	10.177.64.105	10.177.112.5	ICMP
#1-(1-18)	[arachNIDS] [local] [snort] ICMP PING NMAP	2006-03-20 17:37:43	10.177.80.45	10.177.112.5	ICMP
#2-(1-61)	[arachNIDS] [local] [snort] ICMP PING NMAP	2006-03-21 09:20:44	10.177.64.105	10.177.112.5	ICMP
#3-(1-100)	[arachNIDS] [local] [snort] ICMP PING NMAP	2006-03-21 15:43:00	10.177.80.4	10.177.112.5	ICMP
#4-(1-104)	[arachNIDS] [local] [snort] ICMP PING NMAP	2006-03-21 16:13:14	10.177.64.105	10.177.112.5	ICMP
#5-(1-166)	[arachNIDS] [local] [snort] ICMP PING NMAP	2006-03-22 09:12:12	10.177.64.105	10.177.112.5	ICMP
#6-(1-233)	[arachNIDS] [local] [snort] ICMP PING NMAP	2006-03-22 14:03:03	10.177.64.105	10.177.112.5	ICMP
#7-(1-263)	[arachNIDS] [local] [snort] ICMP PING NMAP	2006-03-22 15:23:38	10.177.64.105	10.177.112.5	ICMP

ภาพ 132 แสดงเหตุการณ์ของการแจ้งเตือนภัยโปโตคอล ICMP "ICMP PING NMAP" ตามหมายเลขไอพีต้นทางไปยังหมายเลขไอพีปลายทาง

ถือเป็นการแจ้งเตือนภัยที่เป็นแบบ True Positive

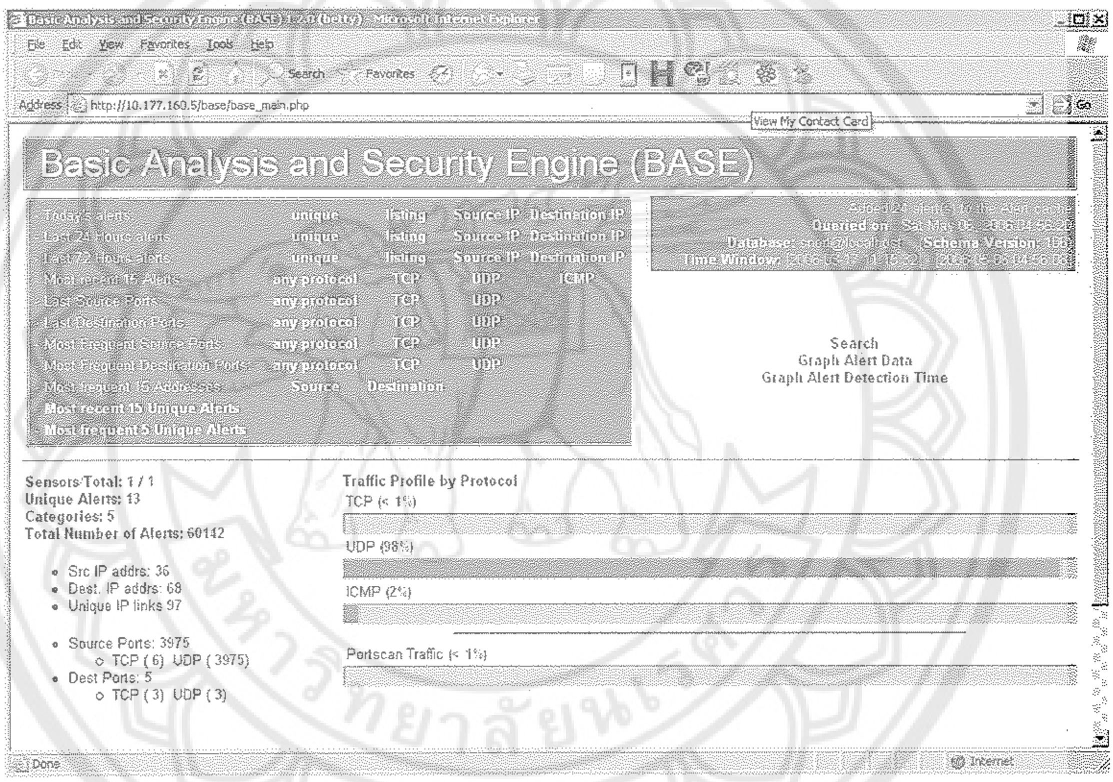
---

[10] http://www.snort.org/pub-bin/sigs.cgi?sid=466

7. สำนักงานคณบดี

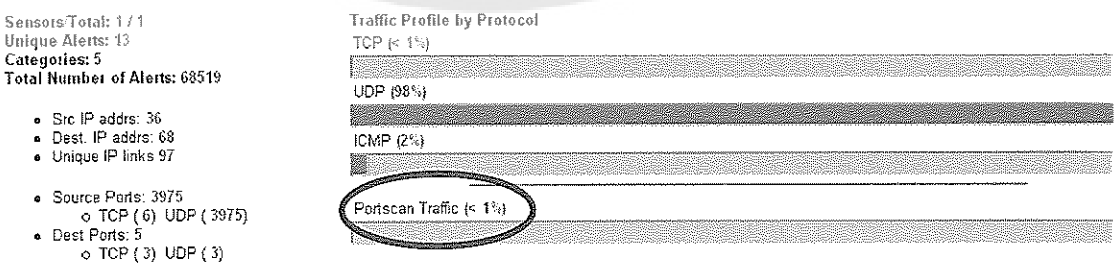
การแบ่งค่าของการตรวจจับออกได้ดังต่อไปนี้

- โปโตคอล TCP มีการแจ้งเตือนภัย 1%
- โปโตคอล UDP มีการแจ้งเตือนภัย 98 %
- โปโตคอล ICMP มีการแจ้งเตือนภัย 2 %
- Portscan Traffic มีการแจ้งเตือนภัย 1 %



ภาพ 133 หน้าต่างหลักภาควิชาวิทยาการคอมพิวเตอร์แสดงการตรวจจับแพ็กเก็ต

7.1 โปรโตคอล TCP มีการแจ้งเตือนภัย 1%



ภาพ 134 โปรโตคอล TCP มีการแจ้งเตือนภัย 1%

เป็นจำนวนทั้งสิ้น 14 ครั้ง

Displaying alerts 1-14 of 14 total

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#0-(1-22273)	[cve] [icat] [cve] [icat] [bugtraq] [bugtraq] [bugtraq] [local] [snort] SNMP request tcp	2006-04-15 00:24:43	10.177.160.39:3737	10.177.160.5:161	TCP
#1-(1-22274)	[cve] [icat] [cve] [icat] [bugtraq] [bugtraq] [bugtraq] [local] [snort] SNMP trap tcp	2006-04-15 00:24:43	10.177.160.39:3738	10.177.160.5:162	TCP
#2-(1-22265)	[cve] [icat] [cve] [icat] [bugtraq] [bugtraq] [bugtraq] [local] [snort] SNMP request tcp	2006-04-15 00:24:37	10.177.160.39:3737	10.177.160.5:161	TCP
#3-(1-22266)	[cve] [icat] [cve] [icat] [bugtraq] [bugtraq] [bugtraq] [local] [snort] SNMP trap tcp	2006-04-15 00:24:37	10.177.160.39:3738	10.177.160.5:162	TCP

ภาพ 135 แสดงการแจ้งเตือนภัยโปรโตคอล TCP เป็นจำนวนทั้งสิ้น 14 ครั้ง

แบ่งแยกตามเหตุการณ์ที่สามารถตรวจจับการบุกรุกได้ ดังต่อไปนี้

Displaying alerts 1-3 of 3 total

< Signature >	< Classification >	< Total # >	Sensor #	< Source Address >	< Dest. Address >	< First >	< Last >
[cve] [icat] [bugtraq] [arachNIDS] [local] [snort] WEB-IIS view source via translate header	web-application-activity	2(0%)	1	1	1	2006-04-12 13:50:35	2006-04-15 00:24:14
[cve] [icat] [cve] [icat] [bugtraq] [bugtraq] [bugtraq] [local] [snort] SNMP request tcp	attempted-recon	6(0%)	1	1	1	2006-04-12 13:52:21	2006-04-15 00:24:43
[cve] [icat] [cve] [icat] [bugtraq] [bugtraq] [bugtraq] [local] [snort] SNMP trap tcp	attempted-recon	6(0%)	1	1	1	2006-04-12 13:52:21	2006-04-15 00:24:43

ภาพ 136 แบ่งแยกตามเหตุการณ์ที่สามารถตรวจจับการบุกรุกได้ (Unique Alerts)

ซึ่งแบ่งออกได้ 3 เหตุการณ์

7.1.7 เหตุการณ์ที่ 1 "WEB-IIS view source via translate header" เป็นจำนวนทั้งสิ้น 2 ครั้ง

Displaying alerts 1-1 of 1 total

< Signature >	< Classification >	< Total # >	Sensor #	< Source Address >	< Dest. Address >	< First >	< Last >
[cve] [icat] [bugtraq] [arachNIDS] [local] [snort] WEB-IIS view source via translate header	web-application-activity	2(0%)	1	1	1	2006-04-12 13:50:35	2006-04-15 00:24:14

ภาพ 137 โปโตคอล TCP WEB-IIS view source via translate header เป็นจำนวนทั้งสิ้น 2 ครั้ง

คำอธิบาย

เป็นการแจ้งเตือนภัยที่มีข้อความแจ้งว่า "WEB-IIS view source via translate header" ช่องโหว่ของ Web Server และ Services ที่ใช้งาน โดยปกติมักติดตั้ง Web Server หรือ HTTP Server ในแบบ Default คือไม่ได้แก้ไขค่าเริ่มต้นต่างๆ ที่มากับตัว Web Server ทำให้เกิดช่องโหว่ที่แฮกเกอร์สามารถนำมาใช้ได้ ระบบอาจเกิดปัญหาเช่น ปัญหา DoS Attack ทำให้ Web Server ไม่สามารถ

ทำงานได้ หรือปัญหาการถูกโจมตีจนแฮกเกอร์สามารถ "ยึด" หรือ "Compromised" เครื่อง Web Server นั้นได้ และ สามารถเปลี่ยนหน้าเว็บเพ็จ ตลอดจนสามารถก๊อบปี้ไฟล์ข้อมูลได้

ช่องโหว่มักเกิดขึ้นเป็นประจำกับ Web Server IIS ของ Microsoft Windows NT/2000 ปกติเป็นเวอร์ชัน 3.0, 4.0 และ 5.0 ตามลำดับ สำหรับเวอร์ชัน 6.0 ที่มากับ Windows Server 2003 มีการปิดกั้นช่องโหว่ต่างๆ มาอย่างดีเมื่อเทียบกับเวอร์ชันก่อนหน้านี้ สำหรับ Apache Web Server ที่ทำงานบน Microsoft Windows ก็มีช่องโหว่เช่นกัน

วิธีการแก้ปัญหา

การลง "Patch" "Hotfix" หรือ อัพเดท Services Pack ล่าสุดของไมโครซอฟท์ เป็นทางออกที่ดีที่สุดในการป้องกันปัญหานี้ การติดตั้ง "Host-based IDS/IPS" ก็เป็นทางออกอีกทางหนึ่ง นอกจากนี้การติดตั้ง "Network-based IDS/IPS" ในลักษณะ In-line ก็สามารถช่วยได้ การเปลี่ยนแปลงค่า Default ต่างๆ หลังการติดตั้งก็เป็นเรื่องที่ต้องทำเช่นกัน รวมถึงการเก็บ Log File ในลักษณะ Remote Log โดยส่ง Log ไปเก็บที่ "Centralized Log Server" ก็เป็นแนวคิดที่ดีเพื่อเราสามารถจะตรวจสอบได้ภายหลังจากการโจมตีโดยไวรัสหรือแฮกเกอร์ การเปลี่ยนจาก IIS 5.0 มาใช้ IIS 6.0 ก็เป็นแนวทางที่ดี แต่ต้องดูเรื่อง "Compatibility" ของ Web Application ด้วย

สามารถอ่านและวิธีการป้องกันเพิ่มเติมได้ที่

http://www.microsoft.com/technet/security/bulletin/MS00-058.mspx

ถือเป็นการแจ้งเตือนภัยที่เป็นแบบ True Positive

7.1.2 เหตุการณ์ที่ 2 "SNMP request tcp" เป็นจำนวนทั้งสิ้น 6 ครั้ง

7.1.3 เหตุการณ์ที่ 3 "SNMP trap tcp" เป็นจำนวนทั้งสิ้น 6 ครั้ง

[cve] [icat] [cve] [icat] [bugtraq] [bugtraq] [bugtraq] [local] [snort] SNMP request tcp	attempted-recon	6(0%)	1	1	1	2006-04-12 13:52:21	2006-04-15 00:24:43
[cve] [icat] [cve] [icat] [bugtraq] [bugtraq] [bugtraq] [local] [snort] SNMP trap tcp	attempted-recon	6(0%)	1	1	1	2006-04-12 13:52:21	2006-04-15 00:24:43

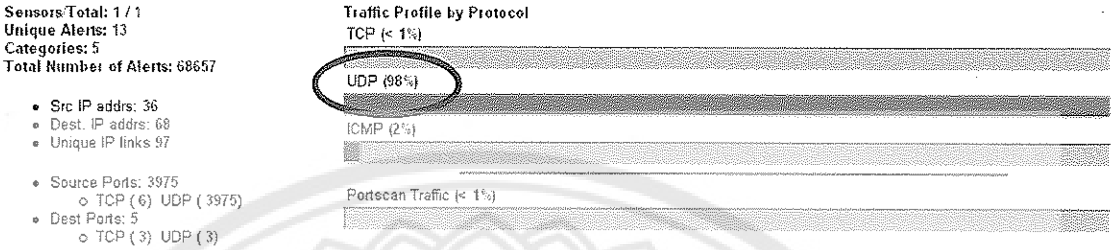
ภาพ 138 โปโตคอล TCP "SNMP request tcp" และ "SNMP trap tcp" จำนวนอย่างละ 6 ครั้ง

คำอธิบาย

เป็นช่วงโหว่ SNMP Service สามารถย้อนไปอ่านรายละเอียดได้ที่ในหน้าที่ 10-5

ถือเป็นการแจ้งเตือนภัยที่เป็นแบบ True Positive

7.2 โปรโตคอล UDP มีการแจ้งเตือนภัย 98%



ภาพ 139 แสดง โปรโตคอล UDP มีการแจ้งเตือนภัย 98%

เป็นจำนวนทั้งสิ้น 67432 ครั้ง

Displaying alerts 1-50 of 67432 total

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto
#0-(1-68691)	[cve] [icat] [cve] [icat] [cve] [icat] [bugtraq] [bugtraq] [bugtraq] [local] [snort] SNMP public access udp	2006-05-06 16:51:16	10.177.160.253:1662	255.255.255.255:161	UDP
#1-(1-68692)	[cve] [icat] [cve] [icat] [bugtraq] [bugtraq] [bugtraq] [local] [snort] SNMP request udp	2006-05-06 16:51:16	10.177.160.253:1662	255.255.255.255:161	UDP
#2-(1-68693)	[cve] [icat] [cve] [icat] [bugtraq] [bugtraq] [bugtraq] [local] [snort] SNMP Broadcast request	2006-05-06 16:51:16	10.177.160.253:1662	255.255.255.255:161	UDP

ภาพ 140 แสดงการแจ้งเตือนภัยโปรโตคอล UDP เป็นจำนวนทั้งสิ้น 67432 ครั้ง

แบ่งแยกตามเหตุการณ์ที่สามารถตรวจจับการบุกรุกได้ ดังต่อไปนี้

Displaying alerts 1-6 of 6 total

< Signature >	< Classification >	< Total # >	Sensor #	< Source Address >	< Dest. Address >	< First >	< Last >
[cve] [icat] [cve] [icat] [cve] [icat] [bugtraq] [bugtraq] [bugtraq] [local] [snort] SNMP public access udp	attempted-recon	22729(33%)	1	7	7	2006-03-17 11:15:32	2006-05-06 16:52:48
[cve] [icat] [cve] [icat] [bugtraq] [bugtraq] [bugtraq] [local] [snort] SNMP request udp	attempted-recon	22741(33%)	1	7	7	2006-03-17 11:15:32	2006-05-06 16:52:48
[cve] [icat] [cve] [icat] [bugtraq] [bugtraq] [bugtraq] [bugtraq] [local] [snort] SNMP private access udp	attempted-recon	6(0%)	1	1	1	2006-03-17 11:15:46	2006-03-17 11:15:57
[local] [snort] SCAN UPnP service discover attempt	network-scan	36(0%)	1	2	1	2006-03-17 11:36:34	2006-03-17 14:05:38
[nessus] [local] [snort] MS-SQL ping attempt	misc-activity	20(0%)	1	5	1	2006-03-18 09:18:17	2006-05-06 10:03:55
[cve] [icat] [cve] [icat] [bugtraq] [bugtraq] [bugtraq] [local] [snort] SNMP Broadcast request	attempted-recon	21918(32%)	1	5	1	2006-03-20 08:27:40	2006-05-06 16:52:48

ภาพ 141 แบ่งแยกตามเหตุการณ์ที่สามารถตรวจจับการบุกรุก (Unique Alerts)

สามารถแบ่งออกได้ 6 เหตุการณ์ดังต่อไปนี้

7.2.1 เหตุการณ์ที่ 1 "SNMP public access udp" จำนวนทั้งสิ้น 22752 ครั้ง

7.2.2 เหตุการณ์ที่ 2 "SNMP request udp" จำนวนทั้งสิ้น 22764 ครั้ง

7.2.3 เหตุการณ์ที่ 3 "SNMP private access udp" จำนวนทั้งสิ้น 6 ครั้ง

7.2.4 เหตุการณ์ที่ 4 "SNMP Broadcast request" จำนวนทั้งสิ้น 21952 ครั้ง

คำอธิบาย

เป็นช่วงโหว่ SNMP Service สามารถย้อนไปอ่านรายละเอียดได้ที่ในหน้าที่ 10-5

ถือเป็นการแจ้งเตือนภัยที่เป็นแบบ True Positive

แต่เนื่องจาก

Simple Network Managament Protocol (SNMP) ถูกนำมาใช้งานอย่างแพร่หลายในปัจจุบัน เพื่อการเฝ้าตรวจและปรับแต่งค่าอุปกรณ์เกือบทุกชนิดที่สามารถทำงานผ่านโพรโตคอล TCP/IP ได้ โพรโตคอล SNMP ถูกนำไปใช้งานอย่างกว้างขวางและมีการทำงานข้ามแพลตฟอร์มต่างๆ ของเครือข่าย ประโยชน์หลักของโพรโตคอล SNMP คือสามารถใช้เป็นวิธีการหนึ่งในการปรับแต่งการทำงานและจัดการอุปกรณ์ เช่น เครื่องพิมพ์ (พรินเตอร์) เราเตอร์ สวิตช์ เป็นต้น หรือใช้ในการส่งค่าอินพุตไปยังบริการที่ทำหน้าที่เฝ้าตรวจเครือข่าย

การติดต่อแบบ Simple Network Management ประกอบด้วยการแลกเปลี่ยนข้อความที่มีรูปแบบต่างๆ ระหว่างเครื่องที่ทำหน้าที่บริหาร SNMP (SNMP management station) กับอุปกรณ์เครือข่ายซึ่งมีการเปิดใช้งานซอฟต์แวร์ชนิดที่นิยมเรียกว่าซอฟต์แวร์เอเจนต์ (agent software) วิธีการทำงานของโพรโตคอล SNMP ดังกล่าวนี้ทำให้เกิดช่องโหว่ซึ่งผู้บุกรุกสามารถนำไปใช้โจมตีได้ทั้งจากวิธีการจัดการข้อความที่ถูกส่ง และจากกลไกการพิสูจน์ตัวตนผู้ใช้งานในระหว่างการจัดการข้อความ

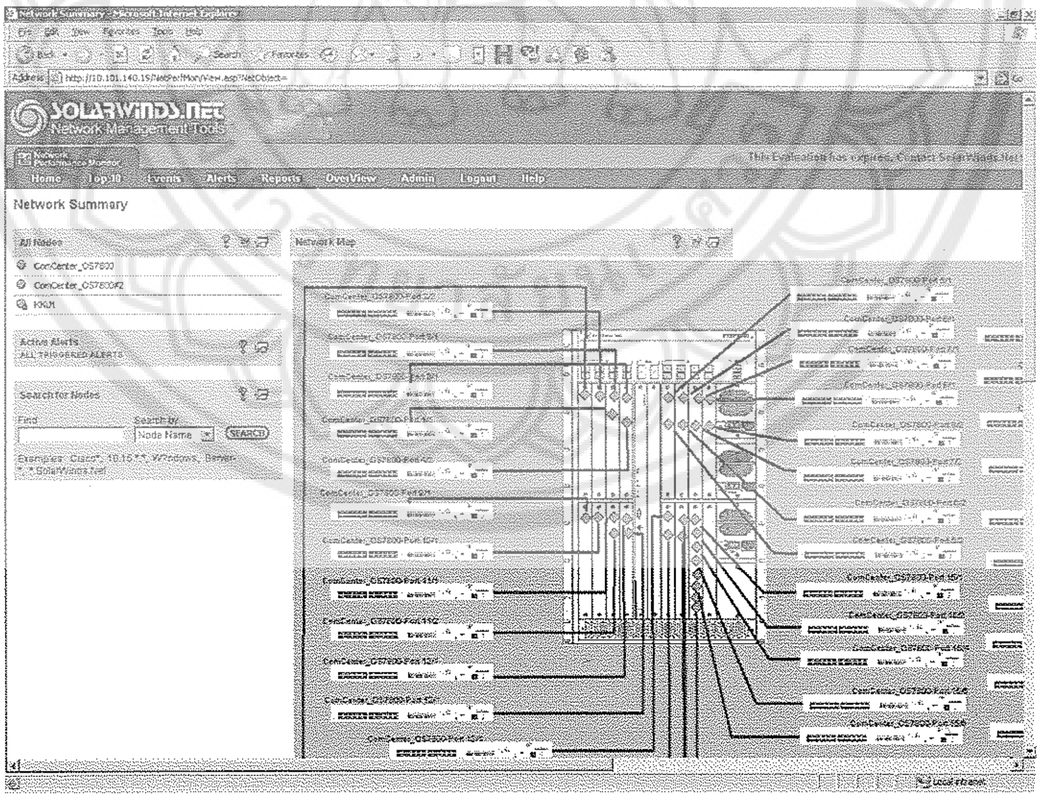
ดังนั้นเมื่อตรวจสอบหมายเลขไอพีแล้วพบว่ามีการติดต่อเพื่อคอยตรวจสอบสถานะระหว่างอุปกรณ์ 2 ชนิดที่เกิดขึ้นของสำนักงานคณบดีดังต่อไปนี้

1. หมายเลขไอพี 10.101.140.19 เปิดบริการ SNMP เข้ามายังเครือข่ายภายใจสำนักงานคณบดี

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#0-(1-1)	[cve] [icat] [cve] [icat] [cve] [icat] [bugtraq] [bugtraq] [bugtraq] [local] [snort] SNMP public access udp	2006-03-17 11:15:32	10.101.140.19:3050	10.177.160.5:161	UDP
#1-(1-5)	[cve] [icat] [cve] [icat] [cve] [icat] [bugtraq] [bugtraq] [bugtraq] [local] [snort] SNMP public access udp	2006-03-17 11:15:34	10.101.140.19:3050	10.177.160.5:161	UDP
#2-(1-10)	[cve] [icat] [cve] [icat] [cve] [icat] [bugtraq] [bugtraq] [bugtraq] [local] [snort] SNMP public access udp	2006-03-17 11:15:36	10.101.140.19:3050	10.177.160.5:161	UDP
#3-(1-13)	[cve] [icat] [cve] [icat] [cve] [icat] [bugtraq] [bugtraq] [bugtraq] [local] [snort] SNMP public access udp	2006-03-17 11:15:39	10.101.140.19:3055	10.177.160.5:161	UDP
#4-(1-16)	[cve] [icat] [cve] [icat] [cve] [icat] [bugtraq] [bugtraq] [bugtraq] [local] [snort] SNMP public access udp	2006-03-17 11:15:41	10.101.140.19:3055	10.177.160.5:161	UDP
#5-(1-19)	[cve] [icat] [cve] [icat] [cve] [icat] [bugtraq] [bugtraq] [bugtraq] [local] [snort] SNMP public access udp	2006-03-17 11:15:43	10.101.140.19:3055	10.177.160.5:161	UDP

ภาพ 142 แสดงหมายเลขไอพี 10.101.140.19 เปิดบริการ SNMP เข้ามายังเครือข่ายภายในสำนักงานคณบดี

เมื่อได้ทำการสำรวจว่าหมายเลขไอพี 10.101.140.19 เป็นอุปกรณ์หรือว่าภัยอันตรายอะไรหรือไม่ พบว่าเป็น Application SOLARWINDS.NET Network Management Tools มีหน้าที่คอยตรวจสอบสถานะอุปกรณ์สวิตช์หลักของคณะวิทยาศาสตร์ที่ตั้งอยู่ที่สำนักงานคณบดี ซึ่งคอยควบคุมจากทางศูนย์คอมพิวเตอร์



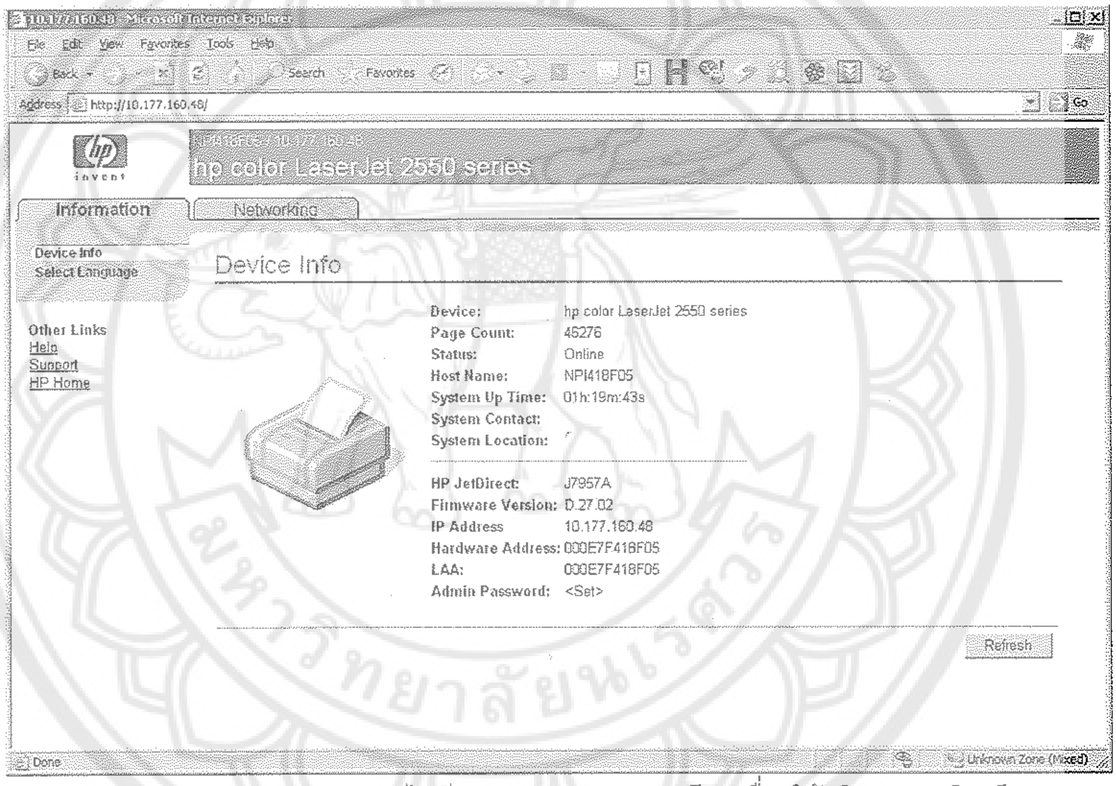
ภาพ 143 SOLARWINDS.NET Network Management Tools

2. หมายเลขไอพี File Server = 10.177.160.253 กับ Printer Server = 10.177.160.48 เพื่อใช้ตรวจสอบสถานการณ์พิมพ์งานของเครื่อง HP รุ่น laserjet 2550tn

Displaying alerts 1-50 of 22760 total

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#0-(1-138)	[cve] [icat] [cve] [icat] [cve] [icat] [bugtraq] [bugtraq] [bugtraq] [local] [snort] SNMP public access udp	2006-03-18 10:58:30	10.177.160.253:1425	10.177.160.48:161	UDP
#1-(1-144)	[cve] [icat] [cve] [icat] [cve] [icat] [bugtraq] [bugtraq] [bugtraq] [local] [snort] SNMP public access udp	2006-03-18 11:24:26	10.177.160.253:1490	10.177.160.48:161	UDP
#2-(1-148)	[cve] [icat] [cve] [icat] [cve] [icat] [bugtraq] [bugtraq] [bugtraq] [local] [snort] SNMP public access udp	2006-03-18 12:10:23	10.177.160.253:1638	10.177.160.48:161	UDP
#3-(1-152)	[cve] [icat] [cve] [icat] [cve] [icat] [bugtraq] [bugtraq] [bugtraq] [local] [snort] SNMP public access udp	2006-03-18 12:20:32	10.177.160.253:1809	10.177.160.48:161	UDP
#4-(1-154)	[cve] [icat] [cve] [icat] [cve] [icat] [bugtraq] [bugtraq] [bugtraq] [local] [snort] SNMP public access udp	2006-03-18 12:33:34	10.177.160.253:2020	10.177.160.48:161	UDP

รูปที่ 144 แสดงการติดต่อกันระหว่างหมายเลขไอพี File Server = 10.177.160.253 กับ Printer Server = 10.177.160.48



ภาพ 145 แสดงหมายเลขไอพี 10.177.160.48 ว่าเป็นเครื่องให้บริการงานพิมพ์

3. หมายเลขไอพี File Server = 10.177.160.253 กับ Printer Server = 10.177.160.16 เพื่อใช้ตรวจสอบสถานการณ์พิมพ์งานของเครื่อง HP รุ่น laserjet 1320

#27-(1-47175)	[cve] [icat] [cve] [icat] [cve] [icat] [bugtraq] [bugtraq] [bugtraq] [local] [snort] SNMP public access udp	2006-05-05 10:48:15	10.177.160.253:2741	10.177.160.16:161	UDP
#28-(1-51785)	[cve] [icat] [cve] [icat] [cve] [icat] [bugtraq] [bugtraq] [bugtraq] [local] [snort] SNMP public access udp	2006-05-05 17:14:15	10.177.160.253:3796	10.177.160.16:161	UDP

ภาพ 146 แสดงการติดต่อกันระหว่างหมายเลขไอพี File Server = 10.177.160.253 กับ Printer Server = 10.177.160.16

7.2.5 เหตุการณ์ที่ 5 “SCAN UPnP service discover attempt” จำนวนทั้งสิ้น 36 ครั้ง

Displaying alerts 1-1 of 1 total

< Signature >	< Classification >	< Total # >	Sensor #	< Source Address >	< Dest. Address >	< First >	< Last >
[local] [snort] SCAN UPnP service discover attempt	network-scan	36(0%)	1	2	1	2006-03-17 11:36:34	2006-03-17 14:05:38

ภาพ 147 แสดง SCAN UPnP service discover attempt จำนวนทั้งสิ้น 36 ครั้ง

คำอธิบาย

เป็นช่วงโหว่ The Universal Plug and Play (UPnP) สามารถย้อนไปอ่านรายละเอียดได้ที่ในหน้าที่ 10-10

ถือเป็นการแจ้งเตือนภัยที่เป็นแบบ True Positive

7.2.6 เหตุการณ์ที่ 6 “MS-SQL ping attempt” จำนวนทั้งสิ้น 20 ครั้ง

Displaying alerts 1-1 of 1 total

< Signature >	< Classification >	< Total # >	Sensor #	< Source Address >	< Dest. Address >	< First >	< Last >
[nessus] [local] [snort] MS-SQL ping attempt	misc-activity	20(0%)	1	5	1	2006-03-16 09:16:17	2006-05-06 10:03:55

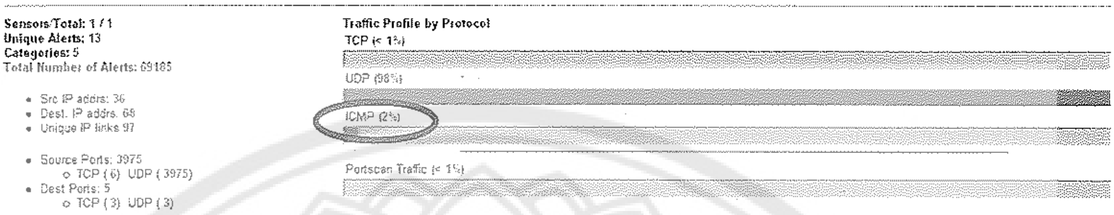
ภาพ 148 แสดง MS-SQL ping attempt จำนวนทั้งสิ้น 20 ครั้ง

คำอธิบาย

MS-SQL ping attempt เป็นช่องโหว่สำคัญของระบบปฏิบัติการ Windows นั้นคือ W3 Microsoft SQL Server สามารถย้อนไปอ่านรายละเอียดได้ที่ในหน้าที่ 10-19

ถือเป็นการแจ้งเตือนภัยที่เป็นแบบ True Positive

7.3 โปรโตคอล ICMP มีการแจ้งเตือนภัย 2%



ภาพ 149 แสดง โปรโตคอล UDP มีการแจ้งเตือนภัย 2%

เป็นจำนวนทั้งสิ้น 1246 ครั้ง

Displaying alerts 1-50 of 1246 total

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#0-(1-49472)	[arachNIDS] [local] [snort] ICMP L3retriever Ping	2006-05-05 14:00:13	10.177.160.27	10.177.160.29	ICMP
#1-(1-35135)	[local] [snort] ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	2006-05-04 18:01:57	10.177.160.5	10.161.204.3	ICMP
#2-(1-35134)	[local] [snort] ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	2006-05-04 18:01:55	10.177.160.5	10.161.204.3	ICMP
#3-(1-35133)	[local] [snort] ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	2006-05-04 18:01:54	10.177.160.5	10.161.204.3	ICMP
#4-(1-	[arachNIDS] [local] [snort] ICMP L3retriever Ping	2006-05-04	10.177.160.12	10.177.160.29	ICMP

ภาพ 150 แสดงการแจ้งเตือนภัยโปรโตคอล UDP เป็นจำนวนทั้งสิ้น 1246 ครั้ง

แบ่งแยกตามเหตุการณ์ที่สามารถตรวจจับการบุกรุกได้ ดังต่อไปนี้

Displaying alerts 1-3 of 3 total

< Signature >	< Classification >	< Total # >	Sensor #	< Source Address >	< Dest. Address >	< First >	< Last >
[local] [snort] ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	misc-activity	1025(1%)	1	1	44	2006-03-17 11:15:32	2006-05-04 18:01:57
[arachNIDS] [local] [snort] ICMP PING NMAP	attempted-recon	2(0%)	1	2	1	2006-03-17 11:16:24	2006-05-02 17:58:44
[arachNIDS] [local] [snort] ICMP L3retriever Ping	attempted-recon	219(0%)	1	22	16	2006-03-20 11:33:26	2006-05-05 14:00:13

ภาพ 151 แบ่งแยกตามเหตุการณ์ที่สามารถตรวจจับการบุกรุก (Unique Alerts)

สามารถแบ่งออกได้ 3 เหตุการณ์ดังต่อไปนี้

7.3.1 เหตุการณ์ที่ 1" ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited " จำนวนทั้งสิ้น 1025 ครั้ง

Displaying alerts 1-1 of 1 total

< Signature >	< Classification >	< Total # >	Sensor #	< Source Address >	< Dest. Address >	< First >	< Last >
[local] [snort] ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	misc-activity	1025(1%)	1	1	44	2006-03-17 11:15:32	2006-05-04 18:01:57

ภาพ 152 แสดงเหตุการณ์ของการแจ้งเตือนภัยโปโตคอล ICMP " ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited " จำนวนทั้งสิ้น 1025 ครั้ง

"ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited " เป็นเหตุการณ์ที่สามารถอธิบายได้ดังข้อความข้างล่างต่อไปนี้

คำอธิบาย

ICMP ชนิดไม่สามารถติดต่อสถานีปลายทาง

เป็นการแจ้งเตือนภัยเกี่ยวกับการป้องกันการโจมตีที่เกิดขึ้นแบบ Denial of Service ซึ่งหาก router ไม่สามารถส่ง datagram ไปยัง router หรือ host ถัดไปได้ router จะตอบกลับด้วย ICMP และใส่รหัสในฟิลด์ code เพื่อบอกสาเหตุของปัญหา

0 — 7	8 — 15	16 — 31
Type = 3	Code = 0 – 15	Checksum
ไม่ใช้งาน (มีค่าเป็น 0)		
Header IP + 64 bit แรกของข้อมูล		

ภาพ 153 ICMP datagram

Code	ความผิดพลาด	ความหมาย
0	Network unreachable	ไปไม่ถึงเครือข่าย
1	Host unreachable	ไปไม่ถึง host
2	Protocol unreachable	ไปไม่ถึง protocol ปลายทาง
3	Port unreachable	ไปไม่ถึง port
4	Fragmentation needed but the Do Not Fragment bit was set	จำเป็นต้องแบ่ง datagram แต่มีการกำหนดไม่ให้แบ่งแยก
5	Source route failed	เส้นทางที่กำหนดล้มเหลว
6	Destination network unknown	ไม่ปรากฏเครือข่ายปลายทาง
7	Destination host unknown	ไม่ปรากฏ host ปลายทาง
8	Source host isolated (obsolete)	
9	Destination network administratively prohibited	มีการป้องกันไม่ให้เข้าเครือข่ายปลายทาง
10	Destination host administratively prohibited	มีการป้องกันไม่ให้เข้า host ปลายทาง

ภาพ 154 Code ของ ICMP

ถือเป็นการแจ้งเตือนภัยที่เป็นแบบ True Positive

7.3.2 เหตุการณ์ที่ 2 "ICMP PING NMAP" จำนวนทั้งสิ้น 2 ครั้ง

Displaying alerts 1-1 of 1 total

< Signature >	< Classification >	< Total # >	Sensor #	< Source Address >	< Dest. Address >	< First >	< Last >
[arachNIDS] [local] [snort] ICMP PING NMAP	attempted-recon	2(0%)	1	2	1	2006-03-17 11:16:24	2006-05-02 17:58:44

ภาพ 155 แสดงเหตุการณ์ของการแจ้งเตือนภัยโปโตคอล ICMP "ICMP PING NMAP"

เหตุการณ์ "ICMP PING NMAP" เป็นเหตุการณ์ที่สามารถอธิบายได้ดังข้อความข้างล่างต่อไปนี้ เป็นการแจ้งเตือนภัยจากการโดน Port scanning ด้วยโปรแกรม NMAP

Displaying alerts 1-2 of 2 total

Source FQDN	< Source IP >	Direction	< Destination IP >	Destination FQDN	Protocol	Unique Dst Ports	Unique Events	Total Events
Unable to resolve address	10.177.80.4	-->	10.177.160.5	*Unable to resolve address*	ICMP	0	1	1
Unable to resolve address	10.177.64.33	-->	10.177.160.5	*Unable to resolve address*	ICMP	0	1	1

ภาพ 156 แสดงเหตุการณ์ของการแจ้งเตือนภัยโปโตคอล ICMP "ICMP PING NMAP" ตามหมายเลขไอพีต้นทางไปยังหมายเลขไอพีปลายทาง

ถือเป็นการแจ้งเตือนภัยที่เป็นแบบ True Positive

7.3.3 เหตุการณ์ที่ 3 “ICMP L3retriever Ping” จำนวนทั้งสิ้น 219 ครั้ง

Displaying alerts 1-1 of 1 total

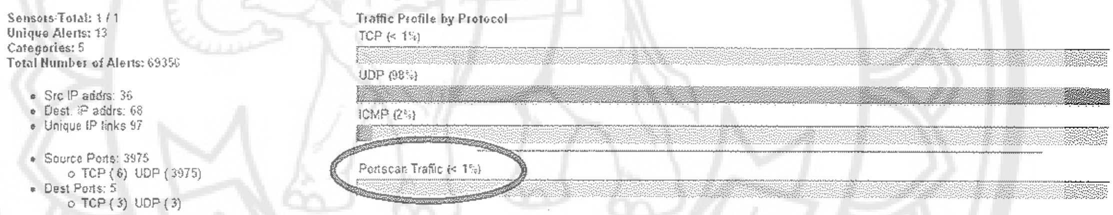
< Signature >	< Classification >	< Total # >	Sensor #	< Source Address >	< Dest. Address >	< First >	< Last >
[arachNIDS] [local] [snort] ICMP L3retriever Ping	attempted-recon	219(0%)	1	22	16	2006-03-20 11:33:26	2006-05-05 14:00:13

ภาพ 157 แสดงเหตุการณ์ของการแจ้งเตือนภัยโปโตคอล ICMP “ICMP L3retriever Ping“

เป็นข้อความแจ้งเตือนภัยของ [11]ICMP echo request จากเครื่องที่ใช้ L3 "Retriever 1.5" ในการสแกน

ถือเป็นการแจ้งเตือนภัยที่เป็นแบบ True Positives

7.4 Portscan Traffic มีการแจ้งเตือนภัย 1%



ภาพ 158 แสดง Portscan Traffic มีการแจ้งเตือนภัย 1%

เป็นจำนวนทั้งสิ้น 1 ครั้ง

Displaying alerts 1-1 of 1 total

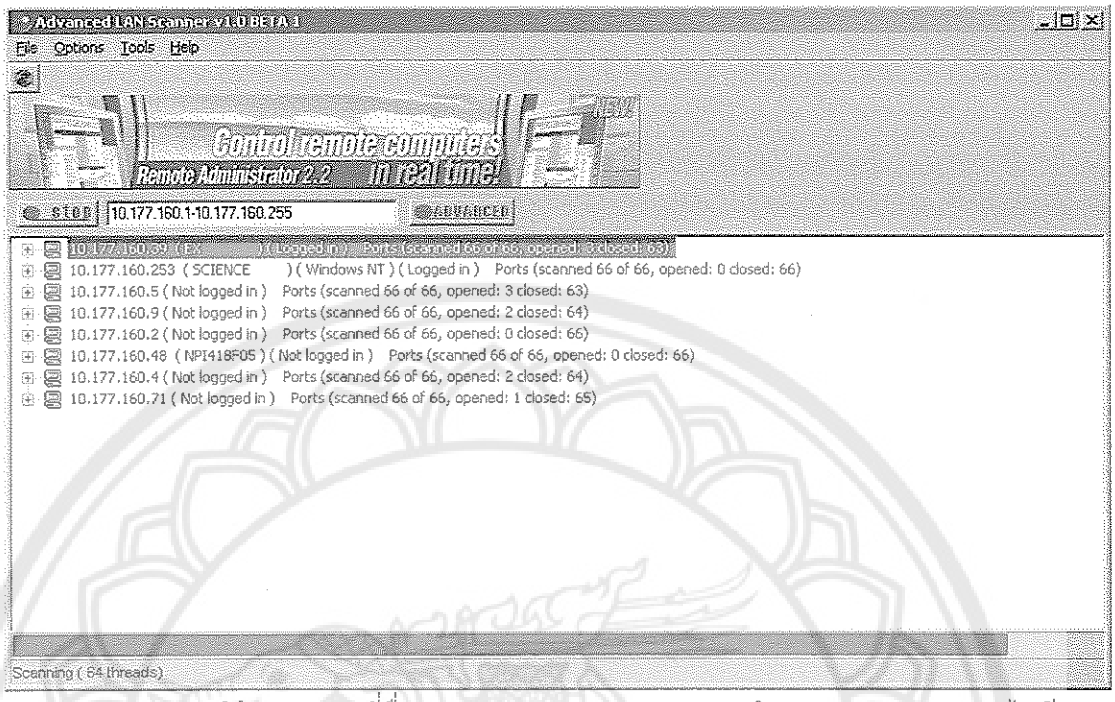
ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#0-(1-22130)	[snort] (portscan) ICMP Sweep	2006-04-12 13:50:11	10.177.160.39	10.177.160.5	Raw IP

ภาพ 159 แสดงการแจ้งเตือนภัยโปรโตคอล UDP เป็นจำนวนทั้งสิ้น 1246 ครั้ง

แบ่งแยกตามเหตุการณ์ที่สามารถตรวจจับการบุกรุกได้ ดังต่อไปนี้

7.4.1 เป็นการใช้ Tool เพื่อ scan หาหมายเลขไอพี ซึ่ง Tool ที่ใช้งานคือ Advanced LAN Scanner

11 http://www.snort.org/pub-bin/sigs.cgi?sid=466



ภาพ 160 การใช้งาน Tool ที่ชื่อว่า Advanced LAN Scannerในการสแกนหมายเลขไอพี

ถือเป็นการแจ้งเตือนภัยที่เป็นแบบ True Positives

การแจ้งเตือนภัยที่ผิดพลาด(False Negative)

การปล่อย Packet ของ port 139 และ 445 ซึ่งเป็น port สำหรับโปรโตคอลของ NetBIOS ของทาง Microsoft ซึ่งได้เกิดขึ้นในเครือข่ายคอมพิวเตอร์คณะวิทยาศาสตร์ มหาวิทยาลัยขอนแก่น

[12]**คำอธิบาย**

หนอน W32/Blaster อาศัยช่องโหว่ใน Microsoft's DCOM RPC interface ซึ่งกล่าวไว้ใน VU#568148 และ CA-2003-16 เพื่อบุกรุกระบบ เมื่อทำการสำเร็จหนอนตัวนี้จะพยายามดาวน์โหลดไฟล์ชื่อ msblast.exe จากโฮสต์ที่ติดเชื้อแล้ว เมื่อได้ไฟล์ดังกล่าวแล้วเจ้าหนอนจะเรียกใช้งานโค้ดนี้และตรวจหาระบบอื่นๆ ที่มีช่องโหว่ให้โจมตีในลักษณะเดียวกันได้อีก เจ้าหนอนตัวทำการโจมตีและแพร่กระจายผ่าน TCP พอร์ต 135 หรืออาจใช้พอร์ต 139 และ 445 ในการโจมตีได้

---

12 ดร. ศิวรักษ์ ศิวโมกษธรรม, CERT Advisory CA-2003-20 W32/Blaster worm, http://thaicert.org/advisory/cert/CA-2003-20.php

ด้วย ดังนั้นควรมีการคำนึงถึงพอร์ตดังกล่าวทั้งหมดนี้เมื่อทำการแก้ไข Microsoft ได้เผยแพร่ข้อมูลเกี่ยวกับช่องโหว่นี้แล้วในเอกสาร Microsoft Security Bulletin MS03-026.

ผลการทดลองในห้องทดลองยืนยันว่าเจ้าหนอนตัวนี้มีความสามารถในโจมตีเว็บไซต์ windowsupdate.com ให้ตกอยู่ในสภาวะไม่สามารถได้ทำงานตามปกติ (denial-of-service) โดยการส่ง TCP SYN จำนวนมาก ขณะนี้ CERT/CC กำลังตรวจสอบหาลักษณะบ่งชี้ที่แน่ชัดของการโจมตีในลักษณะนี้ หากมี tracfic ที่ผิดปกติหรือไม่คาดหมายส่งไปยัง windowsupdate.com แสดงว่าระบบภายใต้ความดูแลของท่านอาจติดเชื้อหนอนดังกล่าว ดังนั้นจึงควรมีการเฝ้าตรวจสอบ traffic ในเครือข่ายภายใต้ความดูแลของท่าน ระบบที่ไม่ได้ใช้บริการของ windowsupdate.com ในการบริหารจัดการกับการนำ patch ต่างๆ มาใช้งานควรจะปิดกั้น traffic ที่จะส่งไปยัง windowsupdate.com แต่ในทางปฏิบัติการปิดกั้นดังกล่าวอาจเป็นไปได้ยาก เนื่องจากไซต์ windowsupdate.com ไม่ได้มีเพียง IP address เดียว การจะปิดกั้น traffic ไปยัง windowsupdate.com ต้องอาศัยความเข้าใจถึงการโครงสร้างและการทำงานของเครือข่ายในความดูแลของท่านรวมถึงกระบวนการแปลงชื่อไซต์ต่างๆ ให้เป็นค่า IP address อย่างละเอียด หากไม่มีความเข้าดังกล่าวอย่างดีแล้วก็ไม่ควรจะทำการปิดกั้น traffic ไปยัง windowsupdate.com ขณะนี้ CERT/CC ได้ประสานงานกับ Microsoft เพื่อตรวจสอบการโจมตีแบบ denial-of-service ในลักษณะดังกล่าวแล้ว

II. ผลกระทบ

ผู้โจมตีจากภายนอกสามารถใช้ช่องโหว่นี้เพื่อเรียกใช้งานโค้ดต่างๆ ได้บนระบบด้วยสิทธิในระดับ Local System และสามารถทำให้ระบบตกอยู่ในสภาวะไม่สามารถทำงานได้ตามปกติ (denial-of-service)

III. การแก้ไข

(หมายเหตุ: วิธีการกู้ระบบ Windows XP systems จากการติดเชื้อหนอน W32/Blaster อย่างละเอียดสามารถศึกษาได้ที่ W32/Blaster Recovery Tech Tip)

นำ patch มาใช้ ควรนำเอา patch ที่ระบุไว้ในเอกสาร Microsoft Security Bulletin MS03-026 มาใช้อย่างรีบด่วนที่สุด เพื่อที่จะแก้ไขช่องโหว่ที่กล่าวไว้ใน VU#568148 . นอกจากนี้ patch ดังกล่าวยังสามารถหาได้ที่ Microsoft's Windows Update service. อย่างไรก็ตามหากยังมีการ

เปิดใช้งาน DCOM RPC ผ่านเครือข่าย ระบบ Windows 2000 อาจยังคงมีความเสี่ยงต่อการถูกโจมตีเพื่อทำให้ตกอยู่ในสภาวะไม่สามารถทำงานตามปกติได้ตามที่ได้กล่าวไว้ใน VU#326746 ดังนั้นนอกจากการนำ patch จาก MS03-026 มาใช้งานแล้ว ผู้ดูแลระบบควรทำการกรองแพ็กเก็ตดังที่จะกล่าวต่อไปในเอกสารนี้ด้วย ในกรณีที่ระบบไม่สามารถเชื่อมต่อเข้ากับเครือข่ายให้นานพอที่จะดาวน์โหลด patch จาก Microsoft มาใช้งานได้ CERT/CC แนะนำให้ปฏิบัติดังต่อไปนี้

1. ถอดสายสัญญาณที่เชื่อมต่อระบบเข้ากับเครือข่าย
2. ตรวจสอบว่าระบบติดเชื้อแล้วหรือไม่

- โดยทั่วไปแล้ว ระบบที่ติดเชื้อจะมี registry key ชื่อ "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\windows auto update" ด้วยค่า msblast.exe ปรากฏอยู่ ในกรณีดังกล่าวให้ทำการลบ registry key นี้โดยใช้ registry editor

3. หากระบบติดเชื้อนี้แล้ว ให้ระงับการทำงานของโค้ด msblast.exe โดยอาศัย Task Manager.
4. ค้นหาไฟล์ชื่อ msblast.exe. และทำลายไฟล์ดังกล่าวให้หมด
5. เลือกปฏิบัติตามคำแนะนำต่อไปนี้เพื่อป้องกันไม่ให้ติดเชื้อก่อนที่จะทำการติดตั้ง patch จาก Microsoft

- ระงับการใช้งาน DCOM ดังที่ระบุไว้ใน MS03-026 และ Microsoft Knowledge Base Article 825750 .
- เรียกใช้งาน Microsoft's Internet Connection Firewall (ICF) หรือโปรแกรมสำหรับกรองแพ็กเก็ตที่โฮสต์เพื่อปิดกั้นการต่อเชื่อมเข้ามายังระบบผ่านพอร์ต 135/TCP. รายละเอียดเกี่ยวกับโปรแกรม ICF สามารถหาอ่านได้ที่ Microsoft Knowledge Base Article 283673

6. เชื่อมต่อเข้ากับเครือข่ายเพื่อนำ pacth ที่ระบุไว้ใน MS03-026 .

บริษัท Trend Micro, Inc. และ Symantec ได้เผยแพร่วิธีปฏิบัติเพื่อแก้ไขปัญหาดังที่กล่าวมาไว้ที่นี้ และ ที่นี้ ตามลำดับ

ระงับการใช้งาน DCOM

หากเป็นไปได้ผู้ดูแลระบบควรจะระงับการใช้ DCOM ตามที่กล่าวไว้ใน MS03-026. ทั้งนี้ทั้งนั้นก็ขึ้นอยู่กับลักษณะการใช้งานของระบบ การงดใช้ DCOM จะช่วยแก้ไขปัญหาช่องโหว่แต่จะมีผลข้างเคียงที่อาจไม่เป็นที่ต้องการ รายละเอียดเพิ่มเติมเกี่ยวกับการระงับ DCOM และผลข้างเคียงสามารถศึกษาได้ที่ Microsoft Knowledge Base Article 825750 .

กรอง traffic ในเครือข่าย

ผู้ดูแลไซต์ควรปิดกั้นการเข้าถึงจากเครือข่ายมายังพอร์ตต่อไปนี้ที่บริเวณเขตแดนของเครือข่าย ซึ่งจะช่วยลดความเสี่ยงต่อการถูกโจมตีจากเครือข่ายภายนอกที่จะทำให้ระบบตกอยู่ในสภาวะไม่สามารถทำงานได้ปกติ พอร์ตที่กล่าวถึงได้แก่

- 69/UDP
- 135/TCP
- 135/UDP
- 139/TCP
- 139/UDP
- 445/TCP
- 445/UDP
- 4444/TCP

ผู้ดูแลระบบควรจะปิดกั้นทั้ง traffic ที่ไหลออกและไหลเข้ามายังพอร์ตเหล่านี้ทั้งที่โฮสต์และในระดับเครือข่าย ทั้งนี้ทั้งนั้นก็ขึ้นอยู่กับลักษณะการทำงานและให้บริการของเครือข่าย ผู้ดูแลระบบสามารถใช้โปรแกรม Microsoft's Internet Connection Firewall ในการปิดกั้น traffic ดังกล่าว

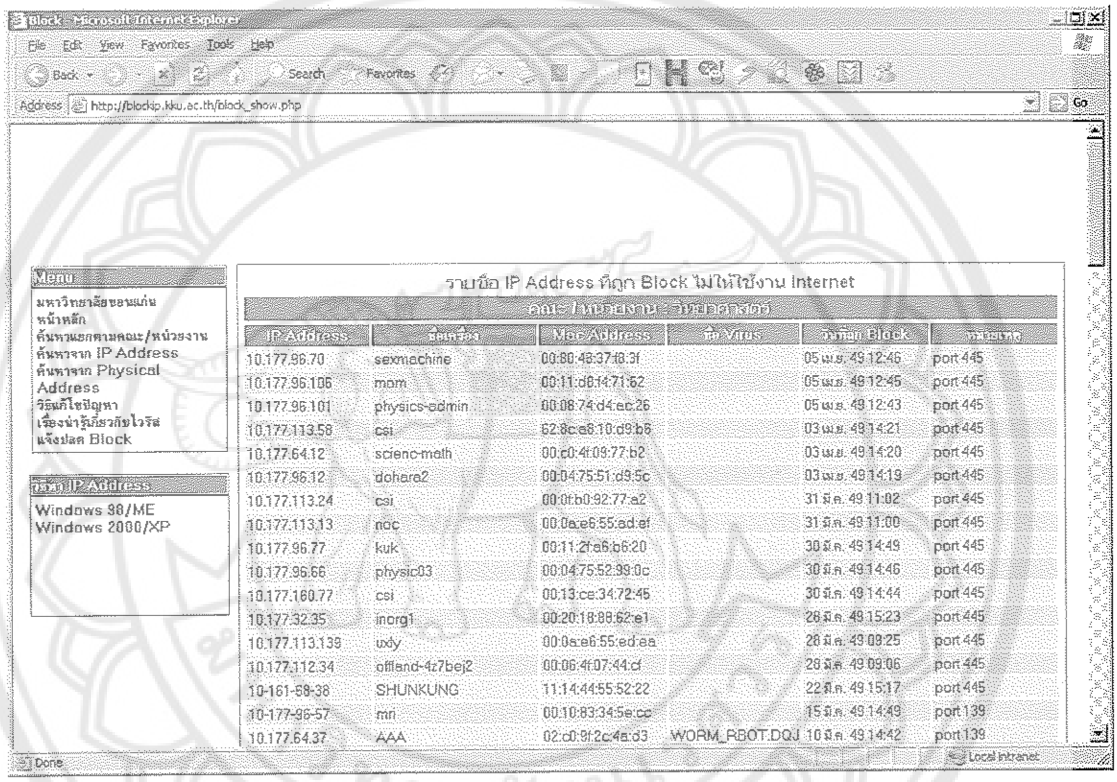
หากไม่สามารถปิดกั้นการเข้าจากภายนอกถึงโฮสต์ทั้งหมดได้ CERT/CC แนะนำให้อนุญาตเฉพาะ traffic ไหลเข้าถึงโฮสต์ที่จำเป็นจริงๆ เท่านั้น ซึ่งเป็นหลักการปฏิบัติที่ CERT/CC แนะนำให้ใช้อยู่แล้ว

เนื่องจากผู้โจมตีสามารถอาศัยช่องโหว่นี้ซึ่งกล่าวไว้ใน VU#568148 ในการเปิด backdoor ไว้บนระบบซึ่งบางครั้งเป็นพอร์ต 4444/TCP, การปิดกั้นการเชื่อมต่อเข้ามาสู่ระบบผ่านพอร์ต TCP ที่ระบบไม่ได้เปิดใช้งานอาจช่วยขัดขวางผู้โจมตีไม่ให้เข้าถึงโฮสต์ที่ติดเชื้อแล้ว

การกู้ระบบที่ติดเชื้อแล้ว

หากระบบภายใต้ความดูแลของท่านได้รับเชื้อหนอนนี้แล้ว โปรดปฏิบัติตามขั้นตอนในเอกสารต่อไปนี้

Steps for Recovering from a UNIX or NT System Compromise



IP Address	[illegible]	Mac Address	[illegible] Virus	[illegible] Block	[illegible]
10.177.96.70	sexmachine	00:80:48:37:f8:3f		05 เม.ย. 49 12:46	port 445
10.177.96.106	mom	00:11:d8:f4:71:62		05 เม.ย. 49 12:45	port 445
10.177.96.101	physics-admin	00:08:74:d4:ec:26		05 เม.ย. 49 12:43	port 445
10.177.113.58	csi	62:8c:e8:10:d9:b6		03 เม.ย. 49 14:21	port 445
10.177.64.12	scienc-math	00:c0:4f:09:77:b2		03 เม.ย. 49 14:20	port 445
10.177.96.12	dohara2	00:04:75:51:d9:5c		03 เม.ย. 49 14:19	port 445
10.177.113.24	csi	00:0f:b0:92:77:a2		31 มี.ค. 49 11:02	port 445
10.177.113.13	noc	00:0a:e6:55:ad:ef		31 มี.ค. 49 11:00	port 445
10.177.96.77	kuk	00:11:2f:a6:b6:20		30 มี.ค. 49 14:49	port 445
10.177.96.66	physic03	00:04:75:52:99:0c		30 มี.ค. 49 14:46	port 445
10.177.160.77	csi	00:13:ce:34:72:45		30 มี.ค. 49 14:44	port 445
10.177.32.35	inorg1	00:20:18:88:62:e1		28 มี.ค. 49 15:23	port 445
10.177.113.139	uxdy	00:0a:e6:55:ed:ea		28 มี.ค. 49 08:25	port 445
10.177.112.34	offland-4z7bej2	00:06:4f:07:44:cf		28 มี.ค. 49 09:06	port 445
10-161-58-38	SHUNKUNG	11:14:44:55:52:22		22 มี.ค. 49 15:17	port 445
10-177-96-57	mri	00:10:83:34:5e:cc		15 มี.ค. 49 14:49	port 139
10.177.64.37	AAA	02:c0:9f:2c:4a:d3	WORM_RBOT.DQJ	10 มี.ค. 49 14:42	port 139

ภาพ 161 หมายเลขไอพีของคณะวิทยาศาสตร์ที่ได้ปล่อยแพ็กเก็ต 139 และ 445 จากทางระบบตรวจจับไวรัสของทางศูนย์คอมพิวเตอร์ มหาวิทยาลัยขอนแก่น

การแก้ไขปรับปรุงกฎของ Snort

- ให้เข้าไปแก้ไขโดยเพิ่มการแจ้งเตือนทุก server snort ที่ตั้งใช้งาน ในไฟล์ /etc/snort/rules/icmp.rules

ข้อความที่เพิ่ม

- alert tcp any any -> any 445 (msg:"NETBIOS SMB-DS DCERPC PnP QueryResConfList exploit attempt"; flow:to_server,established;

content:"|FF|SMB%"; depth:5; offset:4; nocase; content:"&|00|"; within:2; distance:56; content:"|5C 00|P|00|I|00|P|00|E|00 5C 00|"; within:12; distance:5; nocase; content:"|36 00|"; within:2; distance:26; pcre:"/(x00x00.*?)x00xFF.[x04-xFF][x00-xFF]x00$/Rs"; flowbits:isset,netbios.pnp.bind.attempt; reference:cve,CAN-2005-1983; reference:url,www.microsoft.com/technet/security/Bulletin/MS05-039.mspx; classtype:attempted-admin; sid:1000136; rev:2;)

- alert tcp any any -> any 139 (msg:"NETBIOS SMB DCERPC PnP QueryResConfList exploit attempt"; flow:to_server,established; content:"|00|"; depth:1; content:"|FF|SMB%"; depth:5; offset:4; nocase; byte_test:2,^,1,5,relative; content:"&|00|"; within:2; distance:56; content:"|5C|PIPE|5C 00 05 00 00|"; within:10; distance:4; nocase; content:"|36 00|"; within:2; distance:19; pcre:"/(x00x00.*?)x00xFF.[x04-xFF][x00-xFF]x00$/Rs"; flowbits:isset,netbios.pnp.bind.attempt; reference:cve,CAN-2005-1983; reference:url,www.microsoft.com/technet/security/Bulletin/MS05-039.mspx; classtype:attempted-admin; sid:1000138; rev:1;)