ThaiCERT: Thai Computer Emergency Response Team
ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ ประเทศไทย

ชื่อเรื่อง : ความรู้พื้นฐานเกี่ยวกับ Port scanning และวิธีการป้องกัน
เรียบเรียงโดย : ศุภามน วาณิชย์ก่อกุล, สิทธกาณฑ์ ปียมาพรชัย, ชวลิต ทินกรสูติบุตร
เผยแพร่เมื่อ : 10 พฤศจิกายน 2548

กล่าวนำ

Port scanning เป็นกระบวนการในการติดต่อไปที่พอร์ต (port) TCP หรือ UDP ของเครื่องเป้าหมาย มีจุดประสงค์เพื่อตรวจสอบว่ามีบริการใดบ้างบนระบบที่รอรับการเชื่อมต่อ หรืออยู่ในสถานะที่ให้บริการได้

สิ่งที่ผู้ดูแลระบบควรตระหนักถึงคือ การตรวจสอบพอร์ตที่เปิดอยู่นั้นเป็นเรื่องสำคัญในการตรวจสอบประเภทของระบบปฏิบัติการ (Operating System) และแอพพลิเคชั่นที่เปิดใช้งานบนระบบ เนื่องจากระบบปฏิบัติการ หรือเซอร์วิสที่รันอยู่อาจมีช่องโหว่บางอย่างที่อนุญาตให้ผู้ใช้ที่ไม่ได้ผ่านการตรวจสอบสามารถเข้าไปในระบบได้ หรือมีข้อบกพร่องเกี่ยวกับระบบรักษาความมั่นคงปลอดภัยเป็นที่รู้กันดี โดยเฉพาะอย่างยิ่งเซอร์วิสบางเวอร์ชันที่ยังไม่สมบูรณ์ ซึ่งเครื่องมือและเทคนิคในการสแกนพอร์ตได้รับการพัฒนาอย่างต่อเนื่องมาหลายปี

จุดประสงค์หลักการของ Port scanning

- ค้นหาเซอร์วิสที่ทำงานบนโปรโตคอล TCP หรือ UDP ว่ามีเซอร์วิสใดบ้างทำงานอยู่ เช่น http ที่พอร์ต 80 เป็นต้น
- ค้นหาประเภทของระบบปฏิบัติการที่อยู่บนเครื่องเป้าหมาย
- ค้นหาว่ามีแอพพลิเคชั่นใดบ้างที่ทำงานบนเครื่องเป้าหมาย เช่น web server

ก่อนที่จะรู้จักเทคนิคการ Port scanning จำเป็นจะต้องศึกษาการทำงานเบื้องต้นของโปรโตคอล UDP และ TCP
ที่ ความรู้พื้นฐานเกี่ยวกับ โปรโตคอล TCP/IP

ส่วนเนื้อหาโดยรวมของเอกสารนี้ มีดังนี้

รู้จักประเภทของเทคนิคการ Port scanning

TCP/IP Port Numbers

Port Numbers จะเป็น Unsigned Numbers แบบ 16 บิต จะมีพอร์ตได้ทั้งหมด 65536 ports (0-65535)

- Well Known Ports (0 - 1023)
- Registered Ports (1024 - 49151)
- Dynamic and/or Private Ports (49152 - 65535)

Well Known Ports (0-1023) จะเป็นพอร์ตสำหรับ applications ต่างๆ เช่น

- TCP 20 and 21 (File Transfer Protocol, FTP)
- TCP 22 (Secure Shell, SSH)
- TCP 23 (Telnet)
- TCP 25 (Simple Mail Transfer Protocol, SMTP)
- TCP and UDP 53 (Domain Name System, DNS)
- UDP 69 (Trivial File Transfer Protocol, tftp)
- TCP 79 (finger)
- TCP 80 (Hypertext Transfer Protocol, HTTP)
- TCP 110 (Post Office Protocol v3, POP3)
- TCP 119 (Network News Protocol, NNTP)
- UDP 161 and 162 (Simple Network Management Protocol, SNMP)
- UDP 443 (Secure Sockets Layer over HTTP, https)

Non-Standard Port หมายถึงพอร์ตที่มีหมายเลขมากกว่า 1023 ดังตัวอย่าง

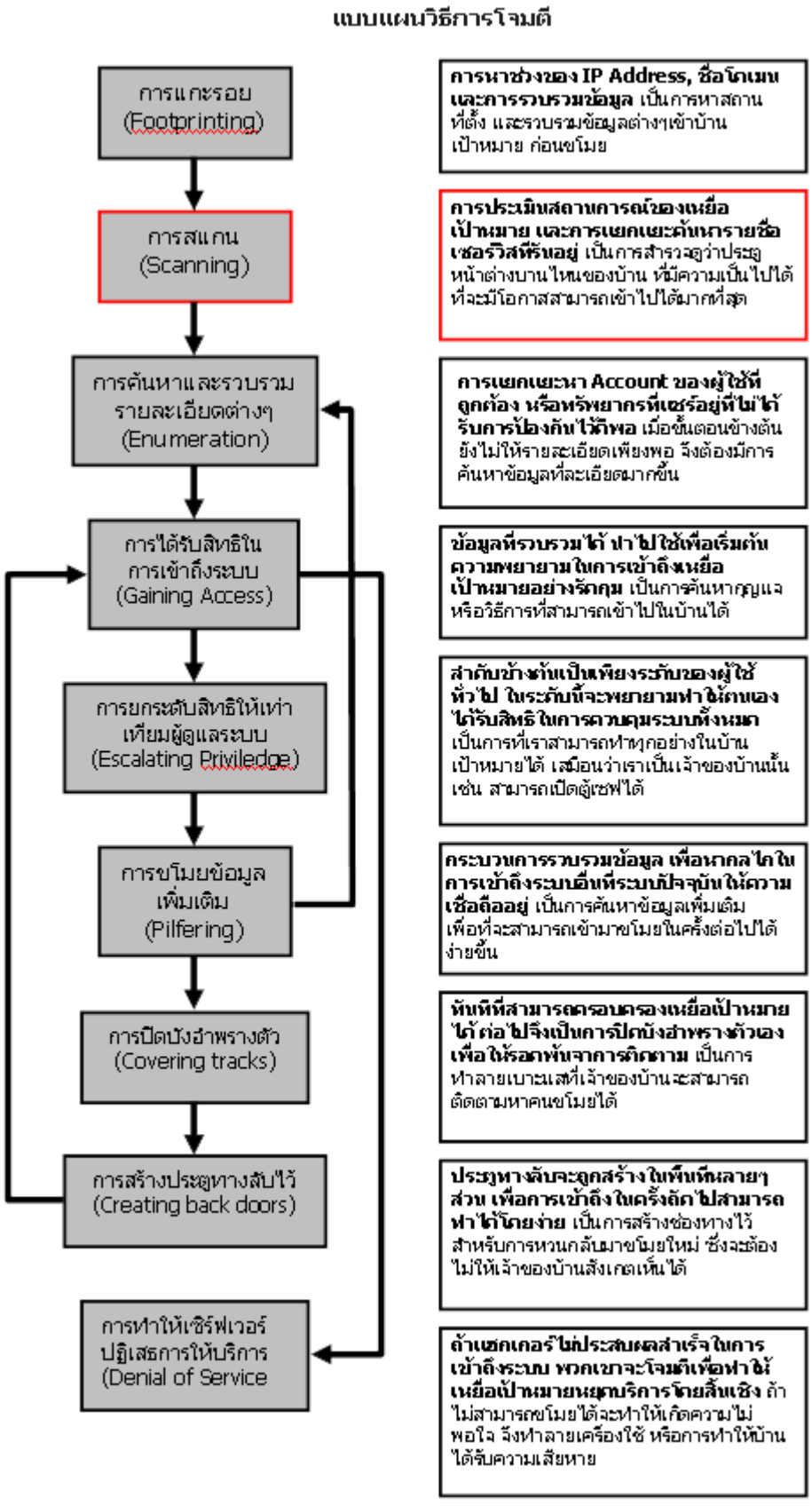
- wins 1512/tcp # Microsoft Windows Internet Name Service
- radius 1812/udp # RADIUS authentication protocol
- yahoo 5010 # Yahoo! Messenger
- x11 6000-6063/tcp # X Window System

Port Scanner ยังสามารถใช้เป็นเครื่องมือในการตรวจจับ Trojan, distributed denial-of-service (DDoS) tools และการกระทำที่ประสงค์ร้ายต่างๆที่เกิดขึ้นบนโฮสต์ (Host) ได้อีกด้วย สามารถดูตัวอย่าง Port List ได้ที่ http://www.garykessler.net/library/is_tools_scan.html

---

แบบแผนวิธีการโจมตี

Port scanning จัดว่าเป็นแผนการขั้นต้นของแฮกเกอร์ในการที่จะโจมตีไปยังเหยื่อเป้าหมาย ซึ่งมีแบบแผนวิธีการโจมตีทั้งหมดดังรูป
แบบแผนวิธีการโจมตี

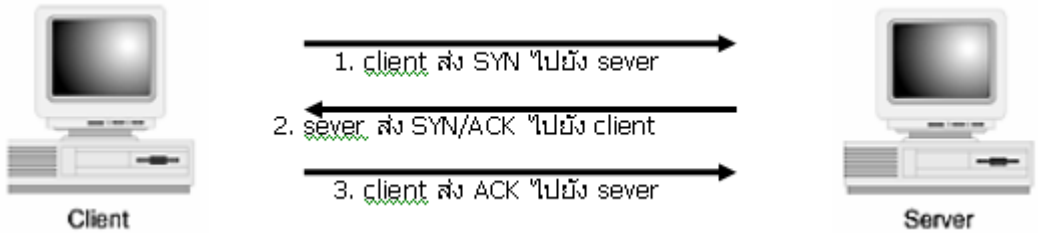


เทคนิคต่าง ๆ ของ Port scanning

ก่อนที่เราจะป้องกัน Port scanning จำเป็นจะต้องเข้าใจถึงเทคนิคของ Port scanning ที่มีอยู่ปัจจุบันก่อนว่ามีลักษณะการทำงานอย่างไร เนื่องจากมีเทคนิคของ Port scanning อยู่มากมายหลายรูปแบบ

เทคนิคของ Port scanning ที่นิยมใช้มีดังนี้

1. **Address Resolution Protocol (ARP) scans** จะตรวจหาอุปกรณ์ที่ทำงานในเครือข่ายโดยการส่งชุด ARP broadcasts Packet และเพิ่มค่าของฟิลด์ที่บรรจุ IP address ของเหยื่อเป้าหมายในแต่ละ broadcast packet การสแกนชนิดนี้จะได้รับผลตอบสนองจากอุปกรณ์ที่มี IP บนเครือข่ายออกมาในรูปแบบของ IP address ของแต่ละอุปกรณ์ การสแกน แบบนี้จึงทำการ map out ได้ทั้งเครือข่ายอย่างมีประสิทธิภาพ แต่มีข้อจำกัดคือสามารถใช้ได้ในเครือข่ายเดียวกันเท่านั้น
2. **The Vanilla TCP connect scan** เป็นเทคนิคการสแกนพอร์ตขั้นพื้นฐานและง่ายที่สุด คือจะใช้ connect system call ของระบบปฏิบัติการไปบนระบบเหยื่อเป้าหมาย ด้วยกลไกมาตรฐานที่เรียกว่า TCP three-way handshake (ดังรูปที่ 1) เพื่อเปิดการเชื่อมต่อไปยังทุกๆ พอร์ตที่เปิดอยู่ การสแกนชนิดนี้สามารถจับได้ง่ายมาก โดยการล็อก (log) ต่าง ๆ ของระบบที่เป็นเหยื่อเป้าหมายจะแสดงการร้องขอการเชื่อมต่อ (connection requests) และข้อความแสดงข้อผิดพลาด (error messages) สำหรับบริการที่ตอบรับการเชื่อมต่อนั้น หรืออาจป้องกันโดยติดตั้งไฟล์วอลล์



TCP's three-way hand shake

3. **The TCP SYN (Half Open) scans** เทคนิคนี้บางครั้งถูกเรียกว่า half open scanning เพราะว่าเป็นการ connectionที่ไม่สมบูรณ์ โดยระบบที่ทำการโจมตีไม่ได้ปิดการเชื่อมต่อที่ได้เปิดไว้ scanner จะส่ง SYN packet ไปยังเหยื่อเป้าหมายและรอการตอบสนอง ถ้าพอร์ตถูกเปิดไว้เป้าหมายก็จะส่ง SYN/ACK กลับมา ซึ่งก็สรุปได้ว่าพอร์ตดังกล่าวอยู่ในสถานะ listening แต่ถ้าพอร์ตถูกปิดอยู่ เป้าหมายก็จะส่ง RST (Reset) กลับมาแทน เทคนิคการสแกนรูปแบบนี้สามารถทำการสแกนเหยื่อเป้าหมายได้อย่างรวดเร็ว และยากต่อการตรวจจับ ปกติเครื่องที่เป็นเหยื่อเป้าหมายจะทำหน้าที่ปิดการเชื่อมต่อที่เปิดไว้ และส่วนใหญ่จะไม่มีระบบการ ล็อกที่เหมาะสมในการตรวจจับการสแกนชนิดนี้
4. **The TCP FIN scan** เทคนิคนี้สามารถที่จะทะลุผ่านไฟล์วอลล์ส่วนใหญ่, packet filters และโปรแกรมตรวจจับการสแกนไปได้โดยไม่ถูกตรวจพบ เพราะระบบที่ทำการโจมตีจะส่ง TCP packets ที่เซตค่า flag FIN เป็น 1 (TCP FIN) ไปยังระบบของเหยื่อเป้าหมาย สำหรับพอร์ตต่าง ๆ ที่ปิดอยู่จะตอบสนองกลับไปด้วย RST ส่วนพอร์ตที่เปิดจะไม่สนใจ packets เหล่านั้นเลย ดังนั้นเครื่องที่ทำการโจมตีก็จะได้ข้อมูลว่ามันได้รับ RST จากพอร์ตไหนบ้างและไม่ได้ RST จากพอร์ตไหนบ้าง (ทำให้ทราบหมายเลขพอร์ตที่ไม่ได้เปิดให้บริการ) โดยปกติแล้ว เทคนิคนี้มักใช้ได้กับเครื่องปลายทางที่รันบนยูนิกซ์
5. **The TCP Reverse Ident scan** เป็นเทคนิคที่สามารถตรวจหาชื่อของเจ้าของแต่ละโพรเซสที่เป็นการเชื่อมต่อด้วย TCP บนเครื่องเหยื่อเป้าหมาย เทคนิคการสแกนชนิดนี้จะทำให้ระบบที่ทำการโจมตีสามารถเชื่อมต่อเข้าไปยังพอร์ตที่เปิดอยู่และใช้ ident protocol ในการค้นหาว่าใครเป็นเจ้าของโพรเซสบนเครื่องเหยื่อเป้าหมายได้
6. **The TCP XMAS** ถูกใช้เพื่อหาพอร์ตบนเครื่องเหยื่อเป้าหมายที่อยู่ในสถานะ listening โดยจะไม่ส่ง TCP packet ทั้ง 3 ตัวซึ่งเป็นที่สังเกตง่าย คือ SYNC-ACK-RST แต่จะใช้ flag เป็น URG, PSH และ FIN ใน TCP header ไปยังพอร์ตของเครื่องเป้าหมาย ทั้งนี้เพื่อหลบหลีกการตรวจจับให้มากที่สุด ซึ่งถ้าพอร์ต TCP ของเครื่องเป้าหมายปิดอยู่ พอร์ตนั้นก็จะส่ง RST กลับมา แต่ถ้าพอร์ตเปิดอยู่ก็จะไม่สนใจ packet นั้นเลย
7. **The TCP NULL scan** เทคนิคนี้จะไม่ใช้ flag ในการสแกนเลย โดยจะส่ง TCP packet ที่มี sequence number แต่ไม่มี flag ออกไปยังเครื่องเป้าหมาย ถ้าพอร์ตปิดอยู่จะส่ง กลับมา RST packet กลับมา แต่ถ้าพอร์ตเปิดอยู่ ก็จะไม่สนใจ packet นั้นเลย โดยทั่วไปแล้ว TCP packet ประเภทนี้จะไม่มีอยู่ในข้อกำหนดของ potocol จึงไม่มีผู้สนใจ นอกจากนี้ยังทำให้ potocol ใน layer ชั้นสูงขึ้นไปไม่ทราบว่ามีการส่ง packet เข้ามาด้วย นอกจากการใช้ packet เหล่านี้เพื่อการสแกนพอร์ตแล้วยังสามารถนำ packet เหล่านี้ไปใช้ในการตรวจสอบระบบปฏิบัติการของเหยื่อเป้าหมายได้อีกด้วย เนื่องจากระบบปฏิบัติการแต่ละแบบจะมีการตอบสนองที่ไม่เหมือนกัน
8. **The TCP ACK scan** เป็นเทคนิคที่ใช้ค้นหาเว็บไซต์ที่เปิดบริการอยู่ แต่ปฏิเสธการตอบสนองต่อ ICMP ping หรือเพื่อค้นหากฎ (rule) หรือนโยบาย (policy) ต่าง ๆ ที่ตั้งไว้ที่ไฟล์วอลล์เพื่อตรวจสอบดูว่าไฟล์วอลล์นั้นๆ ทำหน้าที่แค่เพียงสามารถกรอง packet อย่างง่าย ๆ หรือเป็นไฟล์วอลล์ที่มีความฉลาดพอสมควร และใช้เทคนิคการกรอง packet ขั้นสูง โดยเทคนิคการสแกนแบบนี้จะใช้ TCP packet ที่มี flag เป็น ACK ส่งไปยังพอร์ตเครื่องปลายทาง ถ้าพอร์ตเปิดอยู่ เครื่องเป้าหมายจะส่ง RST กลับมา แต่ถ้าปิดอยู่ก็จะไม่สนใจ packet นั้น
9. **TCP Windows scan** เทคนิคการสแกนนี้จะตรวจสอบพอร์ตที่เปิดอยู่ รวมทั้งตรวจดูว่า พอร์ตใดบ้างที่ถูก filter เอาไว้ไม่ให้ผ่านเข้าไปถึง และพอร์ตหมายเลขใดได้รับการอนุญาตไว้บ้าง โดยอาศัยช่องโหว่จากความผิดปกติบางอย่างในการแจ้งค่า TCP Windows Size ของ TCP/IP protocol
10. **TCP RPC scan** เทคนิคการสแกนนี้ใช้งานได้เฉพาะกับเครื่องปลายทางที่รันบนยูนิกซ์เท่านั้น มันถูกใช้เพื่อตรวจสอบดูว่ามีเซอร์วิสใดทำงานอยู่บนเซอร์วิส RPC บ้าง รวมทั้งตรวจดูเวอร์ชันของเซอร์วิสนั้น และโปรแกรมอื่นที่

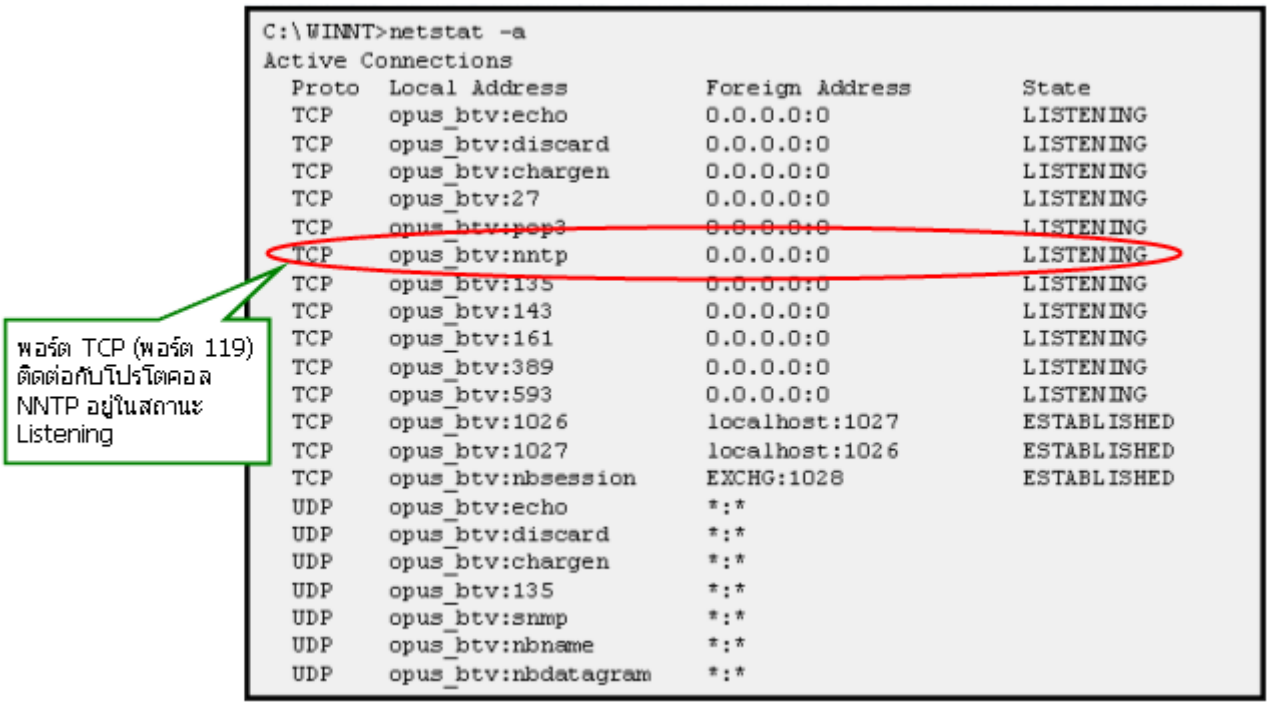
เกี่ยวข้อง

11. **The FTP Bounce Attack** จะใช้ FTP protocol สำหรับสร้างการเชื่อมต่อบริการ FTP ของ ตัวกลาง (proxy) เทคนิคการสแกนแบบนี้ ผู้โจมตีจะสามารถซ่อนตัวอยู่หลัง FTP server และสแกนเป้าหมายอื่น ๆ ได้โดยไม่ถูกตรวจจับ ดังนั้น FTP servers ส่วนใหญ่จะมีการ disable บริการของ FTP เพื่อความปลอดภัยของระบบ
12. **The UDP ICMP Port scanning** ใช้ UDP potocol โดยมันจะส่ง UDP packet ไปยังพอร์ตเป้าหมาย ถ้าพอร์ตที่ปิดอยู่นั้นจะตอบกลับมาด้วย ICMP type PORT UNREACHABLE packet ถ้าพอร์ตนั้นเปิดอยู่มันจะไม่ส่ง packet กลับมา เทคนิคนี้ใช้ในการสแกนหาพอร์ตหมายเลขสูง ๆ โดยเฉพาะในระบบ Solaris แต่จะช้าและไม่น่าเชื่อถือ เนื่องจาก UDO protocol เป็นลักษณะ connectionless คือไม่รับรองว่า packet ที่ส่งไปจะถึงเครื่องปลายทางครบถ้วนหรือไม่
13. **The ICMP ping-sweeping scan** จะใช้คำสั่ง ping เพื่อกวาดดูว่ามีระบบไหนที่เปิดใช้งานอยู่ เครือข่ายส่วนใหญ่จึงมีการกรองหรือ disabled

---

เครื่องมือ Port scanning

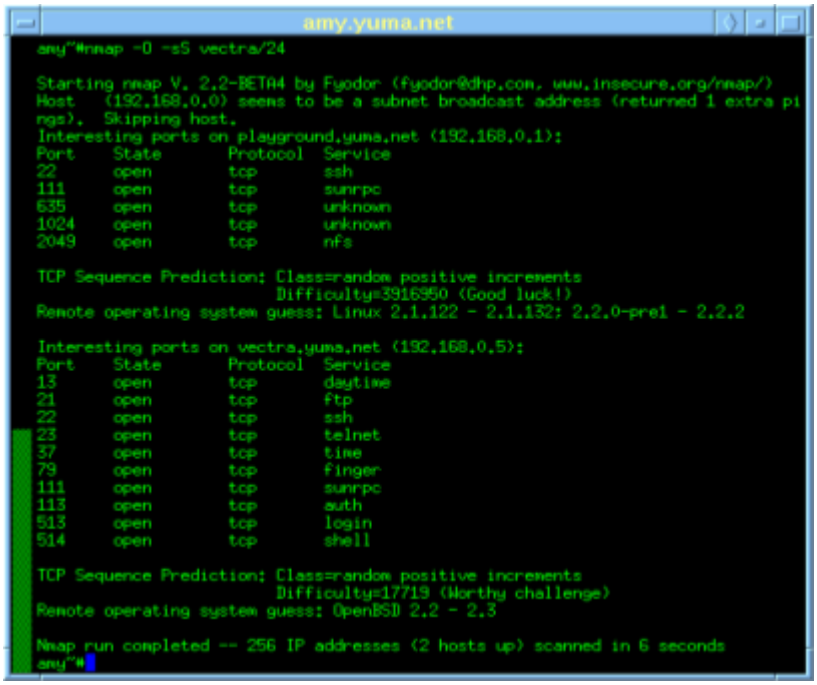
การตรวจสอบ Port ด้วยคำสั่ง netstat
เป็นวิธีที่ง่ายที่สุดที่จะรู้สถานะของพอร์ตของระบบคอมพิวเตอร์ซึ่ง run TCP/IP อยู่ ซึ่งจะแสดงเซอร์วิส ที่ระบบเสนอให้ TCP/IP โฮสต์อื่นๆ ซึ่งสามารถใช้คำสั่งในการดูสถานะของพอร์ตได้ ดังรูปตัวอย่าง



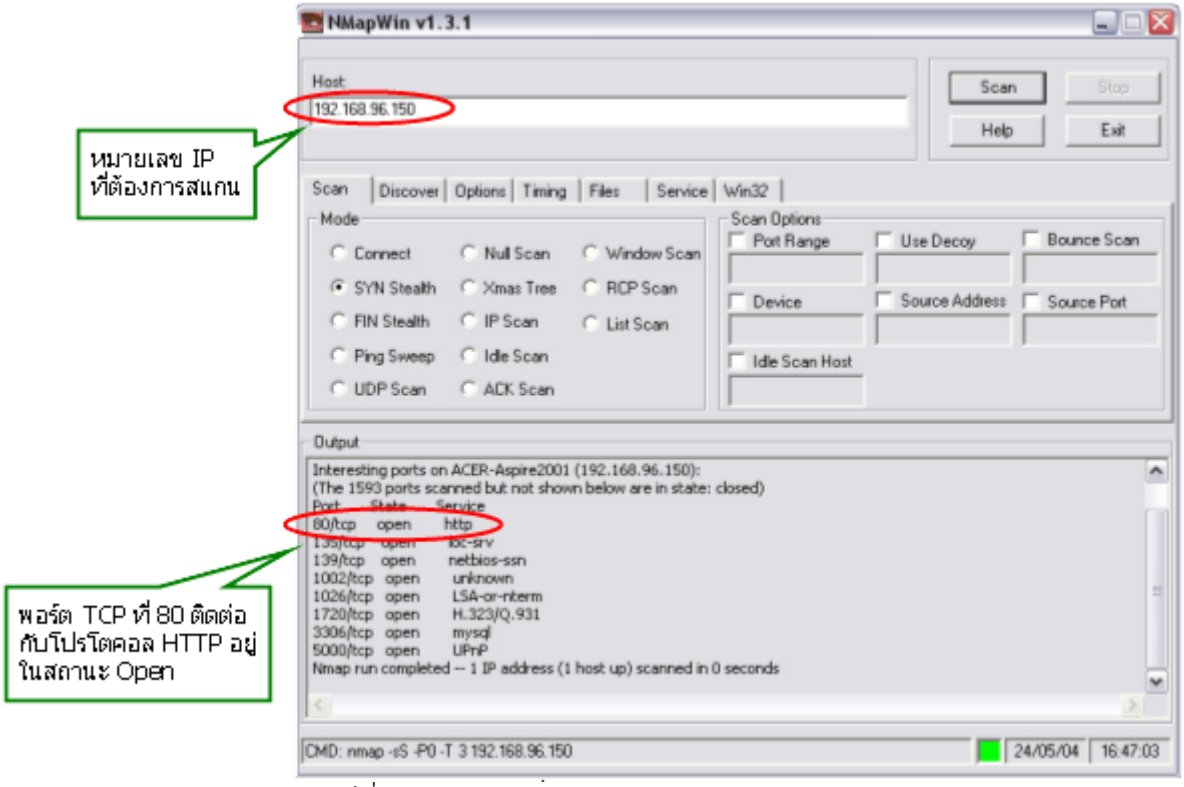

```
C:\WINNT>netstat -a
Active Connections
  Proto  Local Address          Foreign Address        State
  TCP    opus_btv:echo          0.0.0.0:0              LISTENING
  TCP    opus_btv:discard       0.0.0.0:0              LISTENING
  TCP    opus_btv:chargen       0.0.0.0:0              LISTENING
  TCP    opus_btv:27            0.0.0.0:0              LISTENING
  TCP    opus_btv:pop3          0.0.0.0:0              LISTENING
  TCP    opus_btv:nntp          0.0.0.0:0              LISTENING
  TCP    opus_btv:135           0.0.0.0:0              LISTENING
  TCP    opus_btv:143           0.0.0.0:0              LISTENING
  TCP    opus_btv:161           0.0.0.0:0              LISTENING
  TCP    opus_btv:389           0.0.0.0:0              LISTENING
  TCP    opus_btv:593           0.0.0.0:0              LISTENING
  TCP    opus_btv:1026          localhost:1027         ESTABLISHED
  TCP    opus_btv:1027          localhost:1026         ESTABLISHED
  TCP    opus_btv:nbsession     EXCHG:1028             ESTABLISHED
  UDP    opus_btv:echo          *:*
  UDP    opus_btv:discard       *:*
  UDP    opus_btv:chargen       *:*
  UDP    opus_btv:135           *:*
  UDP    opus_btv:snmp          *:*
  UDP    opus_btv:nbname        *:*
  UDP    opus_btv:nbdatagram    *:*
```

รูปที่ 6 netstat command สามารถใช้ได้ทั้ง Linux และ Windows เพื่อที่ ตรวจสอบพอร์ตที่เปิดบน Local Computer

NMAP
เป็นโปรแกรมสำหรับใช้สแกนพอร์ตซึ่งจะใช้หาพอร์ตที่เปิดทั้งหมดใน IP Address ที่กำหนด โดยมีส่วนสำคัญสองส่วนที่จะถูกส่งกลับมาจากโฮสต์คือ การคาดเดาที่ค่อนข้างแน่นอนของลำดับพอร์ต TCP ,UDP และระบบปฏิบัติการของโฮสต์



รูปที่ 7 โปรแกรม NMAP ที่อยู่บน Linux/Unix.



รูปที่ 8 NMAP graphical front end บน Windows

การป้องกัน Port scanning

การตรวจจับการ Port scanning เป็นวิธีที่ดีอีกวิธีหนึ่งในการที่จะช่วยให้ผู้ดูแลระบบคาดการณ์ได้ว่าจะเกิดการโจมตีระบบขึ้นเมื่อไหร่ และโดยใคร ถ้าสามารถป้องกันการ Port scanning ได้ เปรียบเสมือนสามารถสกัดกั้นบันไดขั้นแรกของแฮกเกอร์ได้ ซึ่งปัจจุบันยังไม่มีวิธีการป้องกันการ Port scanning ที่แน่นอน

วิธีการป้องกัน Port Scanning แบ่งเป็นดังนี้
A. ระบบปฏิบัติการ Linux
B. ระบบปฏิบัติการ Windows

A. บนระบบปฏิบัติการ Linux

แบ่งเป็น 2 ลักษณะ ดังนี้

• Prevention

1. การปิดเซอร์วิสที่ไม่จำเป็น หมายถึง การปิดบริการที่ไม่จำเป็นหรือไม่ได้ใช้งาน เช่น ถ้ามีการเปิดบริการ เว็บเซิร์ฟเวอร์ ก็ควรจะเปิดพอร์ตสำหรับ http เท่านั้น ซึ่งสามารถทำได้ดังขั้นตอนต่อไปนี้

- เปิดไฟล์ /etc/inet.conf แล้วใส่เครื่องหมาย comment เข้าไปข้างหน้าเซอร์วิสที่ไม่จำเป็น เพื่อไม่ให้สตาร์ทขณะที่ระบบเริ่มบูต
- แก้ไขที่ไฟล์ของ runlevel ในระบบของเราใช้อยู่ ซึ่งอยู่ในไดเรกทอรี /etc/init.d
- นอกจากนี้ระบบที่ใช้อยู่จะต้องไม่ได้กำลังรันในโหมด X11 มิฉะนั้นระบบของคุณก็จะส่ง broadcast ของบริการหมายเลขพอร์ต 6000 ออกไปไม่ว่าคุณจะล็อกอินหรือไม่ก็ตาม

2. การใช้ TCP Wrappers ซึ่งช่วยให้ผู้ดูแลสามารถกำหนดการอนุญาตหรือปฏิเสธการเข้าถึงบริการต่างๆของระบบ โดยอ้างอิงถึง IP address หรือ domain name โปรแกรมนี้จะทำงานร่วมกับไฟล์ /etc/inet.conf โดยเรียก tcpd daemon ก่อนเพื่อจัดบริการเฉพาะให้ใช้งาน เมื่อมีการร้องขอเข้ามา ก็จะตรวจได้จากพอร์ตที่อนุญาตให้เข้ามา วิธีการป้องกันของโปรแกรม TCP Wrappers มีดังนี้

- ตรวจสอบไฟล์ /etc/hosts.allow เพื่อดูว่า IP addresses หรือ domain name นั้น ๆ ว่ามีสิทธิเข้าถึงการบริการของระบบหรือไม่
- ถ้าไม่มีการระบุอยู่ในไฟล์ข้างต้น TCP Wrappers ก็จะไปตรวจสอบที่ไฟล์ /etc/hosts.deny ถ้าไม่มีการระบุไว้อีกหรือมีข้อความเป็น ALL : ALL TCP Wrappers ระบบก็จะไม่สนใจการร้องขอนั้น และทำการปฏิเสธการให้บริการที่ถูกร้องขอมา
- เมื่อระบบถูกสแกนพอร์ต TCP Wrapper จะยังคงอนุญาตให้ประกาศบริการออกไป แต่ scanner จะไม่ได้รับข้อมูลเพิ่มเติมใดๆ จากพอร์ต
- ถ้าเป็นการสแกนที่มาจากโฮสต์หรือ domain ที่ปรากฏอยู่ในไฟล์ the /etc/hosts.allow ระบบจะแสดงรายชื่อพอร์ตที่เปิดอยู่ แต่ถ้าแฮกเกอร์พยายามจะเจาะเข้ามาทางพอร์ตที่เปิดอยู่นั้น TCP Wrapper ก็จะปฏิเสธการเชื่อมต่อที่เข้ามาที่ไม่ได้มาจากโฮสต์หรือ domain ที่ได้รับอนุญาต
- ในเรื่องของการ IP spoofing เมื่อมีการร้องขอเข้ามา TCP Wrappers จะทำ reverse DNS lookup สำหรับ IP address ที่ร้องขอมา ถ้าค้นพบว่ามีชื่อ Domain name ตรงกับ IP address ที่ร้องขอเข้ามา โปรแกรมก็จะอนุญาตการเชื่อมต่อนั้น แต่ถ้า Domain name ไม่ตรงกับ IP address ที่ร้องขอเข้ามา โปรแกรมก้อจะกำหนดว่าเป็นโฮสต์ที่ไม่ได้รับอนุญาต และจะปฏิเสธการเชื่อมต่อนั้น

ข้อเสียของโปรแกรมนี้คือ ไม่สามารถทำการตรวจสอบครอบคลุมทุกๆ บริการได้ เช่น http และ smtp ถ้าทำการตั้งค่าไม่เหมาะสม จะทำให้เสี่ยงต่อการถูกบุกรุกได้

• Detection

3. การใช้ PortSentry ซึ่งพัฒนาโดย Psionic (www.psionic.com) เป็นการตรวจจับการเชื่อมต่อที่ร้องขอเข้ามา และสามารถตั้งค่าไม่ให้สนใจการร้องขอได้ ซึ่งมีวิธีการดังนี้

- ผู้ดูแลระบบสามารถกำหนดได้ว่าจะให้ PortSentry สนใจการเชื่อมต่อเข้ามาที่พอร์ตไหน และจะปฏิเสธการร้องขอไหนบ้าง ซึ่งผู้ดูแลระบบจะต้องกำหนดการการพอร์ตที่ระบบไม่สนับสนุนไว้
- PortSentry ก็จะตรวจจับโดยการใช้ TCP Wrapper และใส่ข้อมูลของผู้บุกรุกที่น่าสงสัยไว้ในไฟล์ /etc/hosts.deny PortSentry
- จะสร้าง default route statement ให้ระบบที่บุกรุก โดยจะทำให้มีการสร้างเส้นทางให้แก่ทุกๆ packets จากระบบที่ทำการบุกรุกไปยังระบบอื่นหรือไม่ก็ไปยังระบบที่ไม่ได้เปิดอยู่ ทำให้เหมือนว่าเครื่องเป้าหมายไม่มีตัวตนอยู่จริง
- PortSentry ตั้งแต่เวอร์ชัน 1.1 ขึ้นไปสามารถจัดระดับความสำคัญของการจัดการต่อการแสกนพอร์ตได้ และยังสามารถรันคำสั่งภายนอกได้ตามต้องการ จึงมีประโยชน์ต่อการสร้างระบบแจ้งเตือน (Alert and Alarm) ในรูปแบบที่ผู้ดูแลระบบสามารถกำหนดขึ้นได้เอง

บนระบบลีนุกซ์ PortSentry สามารถตรวจจับการ Port scanning ด้วย TCP และ UDP ได้ทุกชนิด ขณะที่ระบบ Solaris

สามารถตรวจจับการ Port scanning แบบ TCP Vanilla และ UDP เท่านั้น

4. Snort เป็นเครื่องมือที่ใช้ตรวจจับการบุกรุกทางเครือข่าย (network intrusion detection) โดย Martin Roesch (http://www.snort.org) การทำงานของ Snort จะใช้ไลบรารี (library) พื้นฐานชื่อ libpcab ซึ่งใช้กันโดยทั่วไปในบรรดา network sniffer และ network analyzer ทั้งหลาย โปรแกรม Snort สามารถทำ protocol analysis, content searching/matching, ตรวจจับการบุกรุกและ probe เช่น buffer overflow, stealth port scan, CGI attack, SMB probe, OS Fingerprint และอื่นๆ

นอกจากนี้ยังมีคุณสมบัติในการทำ real-time alerting อีกด้วย นอกเหนือจากการเก็บล็อกไปที่ syslog หรือเก็บแยกไฟล์ต่างหาก และยังสามารถ alert ผ่าน winpopup ผ่านทาง Samba's client ได้อีกด้วย (ต้อง compile ด้วย option --enable-smbalerts)

การติดตั้ง (คอมไพล์และติดตั้งโดยใช้เวอร์ชัน 1.8-RELEASE (Build 43) ติดตั้งบน Linux)[6]
ขยายไฟล์ที่ดาวน์โหลดมา

```
#tar xzf snort-x.x.x.tar.gz -C /usr/local
```

ย้ายไดเรกทอรีไปยังเป้าหมายที่ขยายไป จากนั้นใช้คำสั่ง

```
#./configure (ใช้ ./configure --help เพื่อดู option ทั้งหมด)
#make
#make install
```

โดยปกติ Snort จะเก็บข้อมูลล็อกอยู่ในรูปของล็อกไฟล์คล้ายๆ กับ syslog แต่เราสามารถสั่งให้ Snort เก็บข้อมูลที่ต้องการไว้ใน database เช่น MySQL, PosgrestSQL หรือ MSSQL ได้ เพื่อให้สามารถดึงข้อมูลมาตรวจสอบได้สะดวกยิ่งขึ้นผ่านทางปลั๊กอิน(plug-ins) เช่น ACID
สร้างไดเรกทอรีเพื่อเก็บล็อกไฟล์ของ Snort ทั้งหมดแยกต่างหาก และควรป้องกันไม่ให้บุคคลอื่น access เข้ามาที่ไดเรกทอรีนั้นๆ โดยปกติแล้วจะสร้างไว้ที่ /var/log/snort

```
#mkdir /var/log/snort
#chmod 700 /var/log/snort
```

ทดสอบโปรแกรม
ทดลองรันคำสั่ง snort -? เพื่อแสดง help ของ Snort ทั้งหมด

สร้างไฟล์ configuration และ rules
จริงๆ แล้ว ขั้นตอนนี้จะไม่ถือว่าเป็นการสร้าง เป็นเพียงการประกอบข้อมูลที่ Snort ให้เรามาแล้วนั้น นำมาจัดให้เป็นระเบียบเรียบร้อยเท่านั้นเอง ซึ่งอาจจะไม่จำเป็น ในที่นี้จะสร้างโฟลเดอร์ขึ้นมาที่ /etc/snort เพื่อใช้เก็บ configuration และ rules files ของ Snort ไว้ต่างหาก

```
#mkdir /etc/snort
```

จากนั้นให้ copy ข้อมูล configuration และ rules files จาก source ของ Snort

```
#cd /usr/local/src/snort
#cp snort.conf /etc/snort
#cp *.rules /etc.snort
#cp classification.config /etc/snort
```

แก้ไข /etc/snort/snort.conf
เราจะใช้ไฟล์ snort.conf เป็นไฟล์หลักในการรัน Snort โดยจำเป็นต้องแก้ไขข้อมูลในบางส่วนดังต่อไปนี้ (vi snort.conf)

- แก้ไข HOME_NET ให้เป็น network address ของเครือข่ายที่ต้องการ monitor เช่น var HOME_NET 10.10.10.0/24
- แก้ไขค่า network ip address อื่นให้ตรงกับความต้องการ เช่น SMTP , SQL_SERVERS
- ค่าที่ควรแก้ไขคือ VAR DNS_SERVERS แก้ให้เป็น DNS_Server ที่ใช้ภายในหน่วยงาน เพื่อป้องกัน fault alarm
- สำหรับ parameter อื่นๆ นั้น สามารถหาข้อมูลเพิ่มเติมได้ที่ www.snort.org พร้อมกับคู่มือการเขียน rule (โดยปกติแล้ว ไม่มีความจำเป็นต้องเขียน rule เอง เพียงแต่หมั่นติดตามข่าว rule ใหม่ๆ ที่ www.snort.org เท่านั้น

เอง)

รัน Snort (daemon)
ทดลองรัน /usr/local/bin/snort -c /etc/snort/snort.conf ถ้าไม่มี error ใดๆ แสดงว่าสามารถใช้งานได้ เพียงแต่การใช้งานจริงนั้นจะรันใน daemon mode โดยจะใช้คำสั่งดังนี้
#/usr/local/bin/snort -D -c /etc/snort/snort.conf
สำหรับ options ของ Snort นั้นมีค่อนข้างเยอะ รายละเอียดสามารถดูได้ใน www.snort.org
ถ้าต้องการให้ Snort รันใน daemon mode ทุกครั้งที่บูตเครื่องขึ้นมาก็ให้แก้ไขไฟล์ /etc/rc.local แล้วใส่คำสั่งด้านบนเพื่อให้ Snort ทำงานเมื่อมีการบูตเครื่องใหม่

Log
ก่อนอื่นเราจะมาทำความเข้าใจระบบของ Snort ก่อน ใน rule หนึ่งๆ ของ Snort นั้นจะมี action ให้เลือก 3 ชนิดคือ log, alert, pass ถ้าเลือกเป็น log ข้อมูลจะถูกเก็บลงล็อกไฟล์ (ถ้าไม่ระบุเป็นพิเศษ จะเก็บไว้ที่ /var/log/snort) และถ้าเลือกเป็น alert และรันใน daemon mode ข้อมูลนั้นๆ จะถูก alert ผ่านทางช่องทาง alert ที่กำหนดไว้ เช่น ผ่านทาง syslog หรือ winpopup แต่โดยปกติแล้ว จะถูกเก็บไว้ที่ /var/log/snort/alert และกรณีสุดท้ายถ้าเลือกเป็น pass นั้น packet นั้นจะถูก drop ทิ้งไป

กรณีของเรานั้นรันใน daemon mode และไม่ได้ระบุ path ใดๆ เป็นพิเศษ ดังนั้น ผู้ดูแลระบบจะต้องทำการตรวจสอบ log ที่ /var/log/snort/alert อยู่เสมอ รวมทั้ง log file อื่นๆ ที่อยู่ในโฟลเดอร์เดียวกัน เช่น portscan.log อีกด้วย

B. ระบบปฏิบัติการ Windows
• Prevention

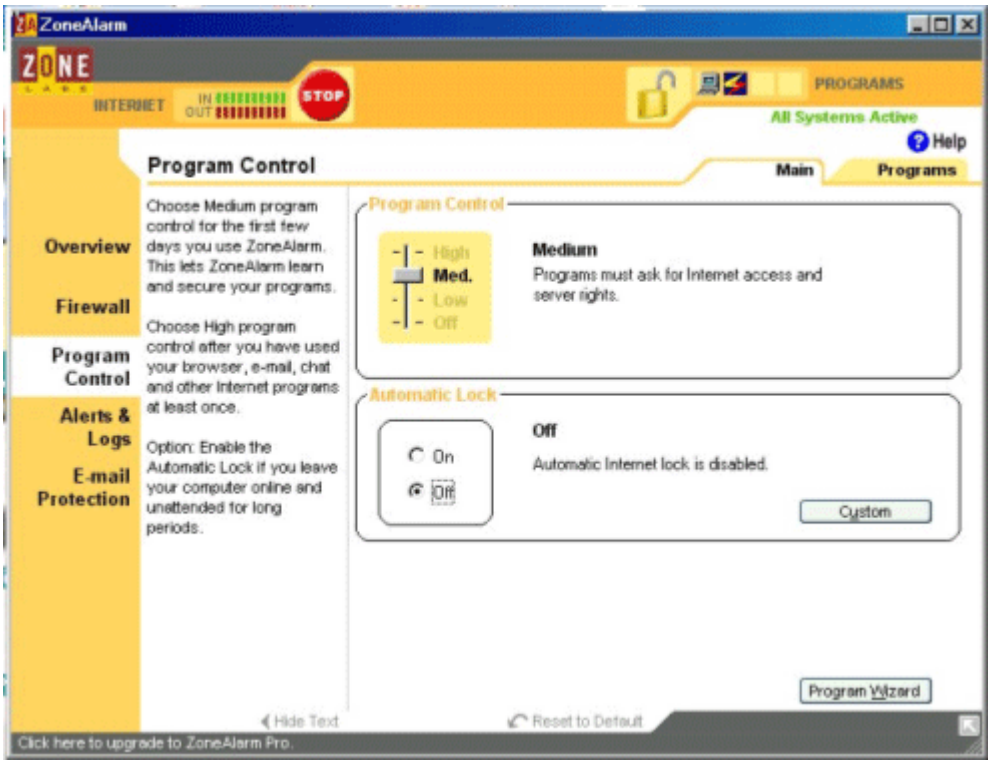
1. การปิดเซอร์วิสที่ไม่จำเป็น ด้วยการไปที Control panel ดับเบิลคลิกที่ไอคอน Services
2. ติดตั้ง Tiny Software (www.tinysoftware.com) ได้จำหน่าย kernel module ของระบบปฏิบัติการ ซึ่งสามารถ filter packet ได้เพื่อช่วยให้สามารถป้องกันพอร์ตสำคัญได้
3. ติดตั้งโปรแกรม ZoneAlarm (www.zonelabs.com) นับเป็น Security Program ที่เหมาะกับ Home User เป็นอย่างมากเนื่องจากมีประสิทธิภาพและความสามารถที่ควบคุมและดูและการทำงานผ่านระบบเครือข่ายไม่ว่าจะเป็นอินเตอร์เน็ตหรือระบบเครือข่าย LAN เป็นโปรแกรมที่ให้ทั้งความสามารถของ Firewall และ IDS ไปด้วยพร้อมๆกัน

โปรแกรม Zonealarm มีข้อดีหลายอย่างทั้งในด้านทางเทคนิคของการทำหน้าที่ Firewall ลักษณะการใช้งาน ขนาดของโปรแกรมที่กะทัดรัด ไม่กินหน่วยความจำและฮาร์ดดิสก์ ใช้งาน CPU น้อยมาก สามารถทำงานได้บน Microsoft Windows ตั้งแต่ Windows 95 ขึ้นไป สำหรับโปรแกรม ZoneAlarm เวอร์ชันปกติอนุญาตให้ผู้ใช้ตามบ้านสามารถใช้งานได้ฟรี ส่วนการใช้งานในทางธุรกิจ หรือเวอร์ชันที่มีความสามารถมากขึ้นคือ ZoneAlarm Pro จะต้องจ่ายค่า license

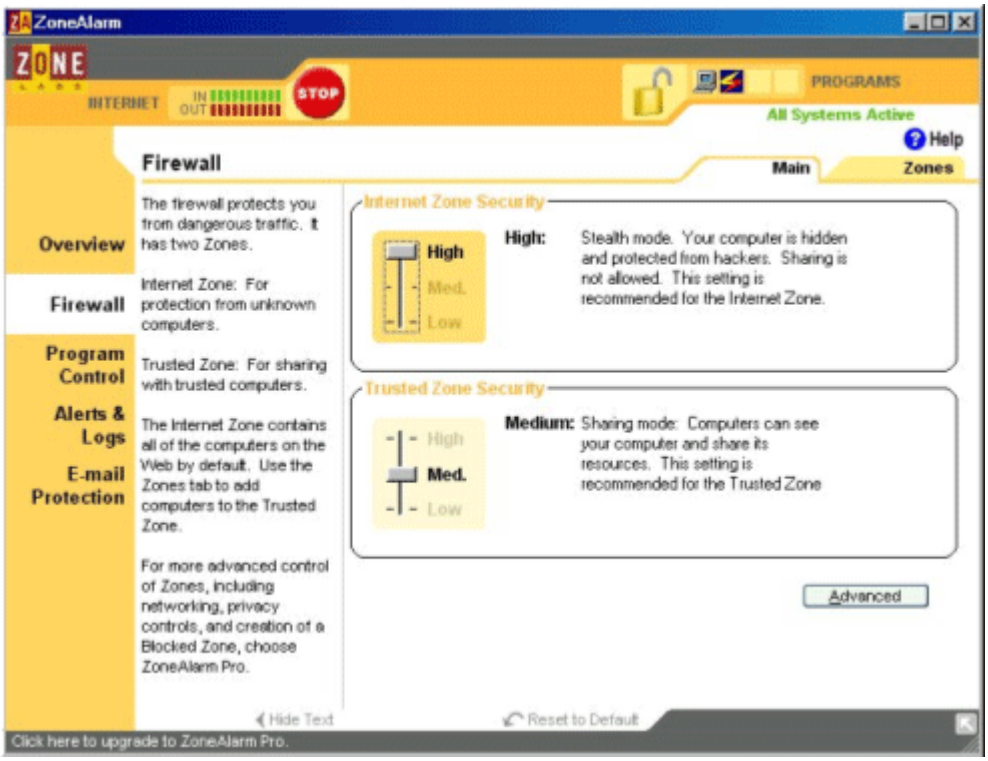
การติดตั้ง
ให้ผู้ใช้ทำการติดตั้งโดยการดับเบิ้ลคลิกไปยังไฟล์ zaSetup_37_098.exe คลิกที่ปุ่ม Next โดยตัวโปรแกรมจะถูกติดตั้งลงบน C:\Program Files\Zone Labs\ZoneAlarm ในหน้าถัดมาให้ผู้ใช้ใส่ชื่อผู้ใช้ ,องค์กร และ อีเมล์ จากนั้นให้คลิกที่ปุ่ม Next ในหน้าถัดมาให้ผู้ใช้ตอบรับข้อตกลงว่าด้วยเรื่องของการใช้งานโปรแกรม ของผู้ผลิต และคลิกที่ Install โปรแกรมจะถูกติดตั้งลงบนโฟลเดอร์ที่ได้เตรียมไว้ หลังจากติดตั้งเสร็จก็จะมีการกรอกแบบสำรวจของทางบริษัทผู้ผลิตโปรแกรม เมื่อกรอกเสร็จคลิกปุ่ม Finish ก็เป็นการสิ้นสุดในการติดตั้งโปรแกรม

การใช้งาน
หลังการติดตั้งเสร็จตัวโปรแกรมก็จะมีการ Introduction ที่ว่าด้วยเรื่องของการใช้งานและ Feature ต่างๆ ให้ผู้ใช้งานทำตามหน้าจอไปเรื่อยครับ ในการใช้งานผู้ใช้สามารถเรียกใช้งานได้โดยเรียกการใช้งานผ่าน Program Files > Zone Labs > ZoneAlarm และเมื่อเข้าสู่ตัวโปรแกรมผู้ใช้งานก็สามารถที่จะตั้งค่าต่างได้เช่น การตั้งระดับความปลอดภัยของ Firewall ทั้งที่ผ่านระบบเครือข่าย LAN และ WAN หรือการตั้งค่าในเมนู Program Control ในการใช้ Application ผ่านระบบเครือข่ายอินเตอร์เน็ต การตั้งค่า Alert เมื่อมีผู้บุกรุก เป็นต้น
ตัวอย่างโปรแกรม ZoneAlarm

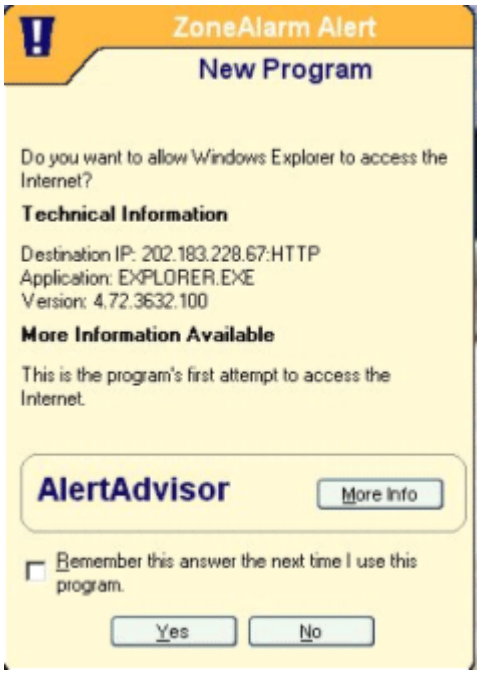
รูปที่ 9 แสดงสถานะในขณะโปรแกรมกำลังทำงาน



รูปที่ 10 แสดงการปรับระดับของโปรแกรมคอนโทรล



รูปที่ 11 แสดงการปรับระดับการรักษาความปลอดภัยในการใช้ internet



รูปที่ 12 แสดงการเตือนเมื่อมีการเปลี่ยนแปลงข้อมูลผ่านพอร์ตต่างๆในเครื่อง

บทสรุป

Port scanning เป็นขั้นตอนที่สำคัญขั้นหนึ่งในการโจมตีของแฮกเกอร์ เพื่อให้สามารถล่วงรู้ได้ว่ามีแอพพลิเคชั่นใดบ้างที่ทำงานอยู่บนเครื่องเป้าหมาย จึงได้มีการคิดค้นเทคนิคสารพัดวิธีในการสแกนพอร์ต ผู้ควบคุมระบบจึงควรติดตั้งเครื่องมือตวจสอบการสแกนพอร์ต และทำการตรวจสอบพอร์ตบนระบบอย่างสม่ำเสมอ ถ้าพบว่ามีพอร์ตที่ไม่จำเป็นต้องใช้ก็ปิดพอร์ตเหล่านั้น เพราะยิ่งมีการบริการเปิดไว้มากก็ยิ่งทำให้ระบบมีจุดอ่อนมากขึ้นไปด้วย ดังนั้นยิ่งผู้ดูแลระบบมีความ

รอบคอบมากเท่าไร ก็ยิ่งทำให้ระบบมีความต้านทานต่อการเจาะเข้ามามากขึ้น และมีโอกาสถูกบุกรุกน้อยลงเท่านั้น

เอกสารอ้างอิง

- [1] McClure, Stuart; Scambray, Joel; Kurtz, George. Hacking Exposed, Network Security Secrets & Solutions. Berekley: Osborne/McGraw Hill, 2001. 38 – 51.
- [2] Andrew S. Tanenbaum. Computer Networks. หน้า32-35 , 432-434 , 463-465
- [3] เรืองไกร รังสิพล. เจาะระบบ TCP/IP : จุดอ่อนของโปรโตคอลและวิธีป้องกัน . บริษัท โปรวิชั่น จำกัด. 2001
- [4] เรืองไกร รังสิพล. เปิดโลก Firewall และ Internet Security . บริษัท โปรวิชั่น จำกัด. , 2002. 293-294
- [5] Christopher Roger. "Port scanning Techniques and the Defense Against Them". October5, 2001., http://www.sans.org/infosecFAQ/audit/port_scan.htm
- [6] ภูวดล ด่านระหาญ ,"การติดตั้ง Snort แบบง่าย", October 3, 2000. , http://www.thaicert.nectec.or.th/paper/ids/snort.php
- [7] Gary C. Kessler. "Port scanning : It's Not Just an Offensive Tool Anymore", May 2001, http://www.garykessler.net/library/is_tools_scan.html
- [8] Port scanning Explained, http://www.auditmypc.com/freescan/readingroom/port_scanning.asp
- [9] http://ale.m5computersecurity.com/tools/
