**ชื่อเรื่อง:** เทคนิคการ Scan Port และวิธีป้องกัน

**ที่มา:** http://www.sans.org/infosecFAQ/audit/port_scan.htm

**แปลและเรียบเรียงโดย:** ศิริวรรณ อภิสิริเดช

**เผยแพร่เมื่อ:** 11 ธันวาคม 2544

**กล่าวนำ**

Port Scanning เป็นหนึ่งในเทคนิคที่โด่งดังที่สุดที่ผู้โจมตีใช้ในการค้นหาบริการที่พวกเขาจะสามารถเจาะผ่านเข้าไปยังระบบได้ โดยปกติแล้วทุก ๆ ระบบที่ต่อเข้าสู่ระบบ LAN หรือระบบอินเทอร์เน็ตจะเปิดบริการทั้งที่อยู่บนพอร์ตที่เป็นที่รู้จักและที่ไม่เป็นที่รู้จัก สำหรับการทำ Port Scanning นั้น ผู้โจมตีจะสามารถค้นหาข้อมูลได้มากมายจากระบบของเป้าหมาย ได้แก่ บริการอะไรบ้างที่กำลังรันอยู่ ผู้ใช้คนไหนเป็นเจ้าของบริการเหล่านั้น สนับสนุนการล็อกอินด้วย anonymous หรือไม่ และบริการด้านเครือข่ายมีการทำ authentication หรือไม่ การทำ Port Scanning ทำได้โดยการส่งข้อความหนึ่งไปยังแต่ละพอร์ต ณ เวลาหนึ่ง ๆ ผลลัพธ์ที่ตอบสนองออกมาจะแสดงให้เห็นว่าพอร์ตนั้น ๆ ถูกใช้อยู่หรือไม่และสามารถทดสอบดูเพื่อหาจุดอ่อนต่อไปได้หรือไม่ Port Scanners มีความสำคัญต่อผู้ชำนาญด้านความปลอดภัยของเครือข่ายมากเพราะว่ามันสามารถเปิดเผยจุดอ่อนด้านความปลอดภัยที่มีความเป็นไปได้ของระบบเป้าหมาย

ถึงแม้ว่า Port Scans สามารถเกิดขึ้นกับระบบของคุณ แต่ก็สามารถตรวจจับได้และก็สามารถใช้เครื่องมือที่เหมาะสมมาจำกัดจำนวนของข้อมูลเกี่ยวกับบริการที่เปิดได้ ทุกๆระบบที่เปิด สู่สาธารณะจะมีพอร์ตหลายพอร์ตที่เปิดและพร้อมให้ใช้งานได้ โดยมีการจำกัดจำนวนพอร์ตที่จะเปิดให้แก่ผู้ใช้ที่ได้รับอนุญาตและปฏิเสธการเข้าถึงมายังพอร์ตที่ปิด

**เทคนิคต่าง ๆ ของ Port Scan**

ก่อนที่คุณจะป้องกัน Port Scans คุณก็จะต้องเข้าใจเสียก่อนว่า Port Scans ทำงานอย่างไร เนื่องจากมีเทคนิคของ Port Scanning อยู่มากมายหลายรูปแบบ ซึ่งมีเครื่องมือ Port Scanning ที่ทำงานโดยอัตโนมัติ เช่น Nmap และ Nessus

การ scan ต่อไปนี้เป็นรูปแบบมาตรฐานสำหรับ Nmap และ Nessus

> **1. Address Resolution Protocol (ARP) scans** จะตรวจหาอุปกรณ์ที่ทำงานในเครือข่ายโดยการส่งชุดของ ARP broadcasts และเพิ่มค่าของฟิลด์ที่บรรจุ IP address ของเป้าหมายในแต่ละ broadcast packet การ scan ชนิดนี้จะได้รับผลตอบสนองจากอุปกรณ์ที่มี IP บนเครือข่ายออกมาในรูปแบบของ IP address ของแต่ละอุปกรณ์ การ scan แบบนี้จึงทำการ map out ได้

ทั้งเครือข่ายอย่างมีประสิทธิภาพ

**2.The Vanilla TCP connect scan** เป็นเทคนิคการ scan แบบพื้นฐานและง่ายที่สุด คือจะใช้ connect system call ของระบบปฏิบัติการไปบนระบบเป้าหมายเพื่อเปิดการเชื่อมต่อไปยังทุก ๆ พอร์ตที่เปิดอยู่ การ scan ชนิดนี้สามารถจับได้ง่ายมาก โดยล็อก (log) ต่าง ๆ ของระบบที่เป็นเป้าหมายจะแสดงการร้องขอการเชื่อมต่อ (connection requests ) และข้อความแสดงข้อผิดพลาด (error messages) สำหรับบริการที่ตอบรับการเชื่อมต่อนั้น

**3.The TCP SYN (Half Open) scans** เทคนิคนี้บางครั้งถูกเรียกว่า half open เพราะว่าระบบที่ทำการโจมตีไม่ได้ปิดการเชื่อมต่อที่ได้เปิดไว้ scanner จะส่ง SYN packet ไปยังเป้าหมายและรอการตอบสนอง ถ้าพอร์ตถูกเปิดไว้เป้าหมายก็จะส่ง SYN/ACK กลับมา แต่ถ้าพอร์ตถูกปิดอยู่ เป้าหมายก็จะส่ง RST กลับมา วิธีการ scan รูปแบบนี้ยากต่อการตรวจจับ ปกติเครื่องที่เป็นเป้าหมายจะทำหน้าที่ปิดการเชื่อมต่อที่เปิดไว้ และส่วนใหญ่จะไม่มีระบบการล็อกที่เหมาะสมในการตรวจจับการ scan ชนิดนี้

**4.The TCP FIN scan** เทคนิคนี้สามารถที่จะทะลุผ่านไฟล์วอลล์ ส่วนใหญ่, packet filters , cละโปรแกรมตรวจจับการ scan ไปได้โดยไม่ถูกตรวจพบ เพราะระบบที่ทำการโจมตีจะส่ง FIN packets ไปยังระบบของเป้าหมาย สำหรับพอร์ตต่าง ๆ ที่ปิดอยู่จะตอบสนองกลับไปด้วย RST ส่วนพอร์ตที่เปิดจะไม่สนใจ packets เหล่านั้นเลย ดังนั้นเครื่องที่ทำการโจมตีก็จะได้ข้อมูลว่ามันได้รับ RST จากพอร์ตไหนบ้างและไม่ได้ RST จากพอร์ตไหนบ้าง

**5.The TCP Reverse Ident scan** เป็นเทคนิคที่สามารถตรวจหาชื่อของเจ้าของแต่ละโพรเซสที่เป็นการเชื่อมต่อด้วย TCP บนเครื่องเป้าหมาย การ scan ชนิดนี้จะทำให้ระบบที่ทำการโจมตีสามารถเชื่อมต่อเข้าไปยังพอร์ตที่เปิดอยู่และใช้ ident protocol ในการค้นหาว่าใครเป็นเจ้าของโพรเซสบนเครื่องเป้าหมายได้

**6.The TCP XMAS** ถูกใช้เพื่อหาพอร์ตบนเครื่องเป้าหมายที่อยู่ในสถานะ listening โดยจะส่ง TCP packet ที่มี flag เป็น URG, PSH และ FIN ใน TCP header ไปยังพอร์ตของเครื่องเป้าหมาย ถ้าพอร์ต TCP ของเครื่องเป้าหมายปิดอยู่ พอร์ตนั้นก็จะส่ง RST กลับมา แต่ถ้าพอร์ตเปิดอยู่ก็จะไม่สนใจ packet นั้นเลย

**7.The TCP NULL scan** เทคนิคนี้จะส่ง TCP packet ที่มี sequence number แต่ไม่มี flag ออกไปยังเครื่องเป้าหมาย ถ้าพอร์ตปิดอยู่จะส่ง กลับมา RST packet กลับมา แต่ถ้าพอร์ตเปิดอยู่ ก็จะไม่สนใจ packet นั้นเลย

**8.The TCP ACK scan** เป็นเทคนิคที่ใช้ค้นหาเว็บไซต์ที่เปิดบริการอยู่ แต่ปฏิเสธการตอบสนองต่อ ICMP ping หรือค้นหากฎ (rule) หรือนโยบาย ( policy) ต่าง ๆ ที่ตั้งไว้ที่ไฟล์วอลล์เพื่อตรวจสอบดูว่าไฟล์วอลล์สามารถกรอง packet อย่างง่าย ๆ หรือเทคนิคชั้นสูง โดยการ scan แบบนี้จะใช้ TCP packet ที่มี flag เป็น ACK ส่งไปยังพอร์ตเครื่องปลายทาง ถ้าพอร์ตเปิดอยู่ เครื่องเป้าหมายจะส่ง RST กลับมา แต่ถ้าปิดอยู่ก็จะไม่สนใจ packet นั้น

**9.The FTP Bounce Attack** ใช้โพรโตคอล ftp สำหรับสร้างการเชื่อมต่อบริการ ftp ของ proxy วิธีการ scan แบบนี้ ผู้โจมตีจะสามารถซ่อนตัวอยู่หลัง ftp server และ scan เป้าหมายอื่น ๆ ได้โดยไม่ถูกตรวจจับ ดังนั้น ftp servers ส่วนใหญ่จะมีการ disable บริการของ ftp เพื่อความปลอดภัยของระบบ

**10.The UDP ICMP port scan** ใช้โพรโตคอล UDP ในการ scan หาพอร์ตหมายเลขสูง ๆ โดยเฉพาะในระบบ Solaris แต่จะช้าและไม่น่าเชื่อถือ

**11.The ICMP ping-sweeping scan** จะใช้คำสั่ง ping เพื่อกวาดดูว่ามีระบบไหนที่เปิดใช้งานอยู่ เครือข่ายส่วนใหญ่จึงมีการกรองหรือ disabled
โพรโตคอล ICMP เพื่อความปลอดภัยของระบบ

**การปกป้องระบบจาก Port Scans**

ถ้าคุณมี server ที่เปิดให้เข้าถึงได้จากภายนอก ระบบก็จะมีความเสี่ยงต่อการถูก scan port อย่างแน่นอน ปัจจุบันนี้ยังไม่มีวิธีที่แน่นอนในการปราบ port scan เลย และศาลก็พิจารณาว่าการทำ port scan นั้นไม่ผิดกฎหมาย เพียงแต่ถ้าผู้โจมตีนำเอาข้อมูลจาก port scan ไปใช้เจาะหรือเปิดพอร์ตของระบบจึงจะถือว่าผิดกฎหมาย ดังนั้นจึงมีคำถามเกิดขึ้นว่า เราจะทำอย่างไรในการจำกัดข้อมูลที่ถูกส่งออกไปจากระบบของเรา?

วิธีหนึ่งที่จะจำกัดการเข้าถึงข้อมูลจากการทำ port scan ก็คือปิดบริการต่าง ๆ ที่ไม่จำเป็นบนระบบ เช่น ถ้าคุณมีการเปิดบริการ web server ก็ควรจะเปิดพอร์ตสำหรับ http เท่านั้น ในระบบ UNIX มีวิธีที่ง่ายที่สุดในการจำกัดข้อมูลที่จะส่งให้ port scan คือ การแก้ไขที่ไฟล์ /etc/inetd.conf โดยยกเลิกบริการที่ไม่จำเป็นออกไป แล้วแก้ไขที่ไฟล์ของ runlevel ที่ระบบของคุณใช้อยู่ ซึ่งอยู่ภายใต้ไดเรกทอรี /etc/init.d นอกจากนี้ระบบของคุณจะต้อง

ไม่ได้กำลังรันในโหมด X11 มิฉะนั้นระบบของคุณก็จะส่ง broadcast ของบริการหมายเลขพอร์ต 6000 ออกไป ไม่ว่าคุณจะล็อกอินหรือไม่ก็ตาม

อีกวิธีหนึ่ง คือ ใช้ TCP Wrappers ซึ่งช่วยให้ผู้ดูแลสามารถกำหนดการอนุญาตหรือปฏิเสธการเข้าถึงบริการต่าง ๆ โดยอ้างอิงถึง IP addresses หรือ domain names โปรแกรม TCP Wrappers ทำงานร่วมกับไฟล์ /etc/inetd.conf ซึ่งทำงานโดยเรียก tcpd daemon ก่อนเพื่อจัดบริการเฉพาะให้ใช้งาน เมื่อมีการร้องขอเข้ามาโดยตรวจได้จากพอร์ตที่อนุญาตให้เข้ามา ก่อนอื่น TCP Wrappers ก็จะตรวจสอบไฟล์ /etc/hosts.allow เพื่อดูว่า IP addresses หรือ domain name นั้น ๆ มีสิทธิเข้าถึงบริการหรือไม่ ถ้าไม่มีการระบุอยู่ในไฟล์นี้ TCP Wrappers ก็จะตรวจสอบที่ไฟล์ /etc/hosts.deny ถ้าไม่มีการระบุไว้อีกหรือมีข้อความเป็น ALL : ALL TCP Wrappers ก็จะไม่สนใจการร้องขอนั้น และไม่อนุญาตให้ใช้บริการที่ถูกร้องขอเข้ามา เมื่อระบบถูก scan port TCP Wrapper จะยังคงอนุญาตให้ประกาศบริการออกไป แต่อย่างไรก็ตาม scanner จะไม่ได้รับข้อมูลเพิ่มเติมใด ๆ จากพอร์ตยกเว้นว่าจะเป็นการ scan มาจาก host หรือ domain ที่ระบุไว้ในไฟล์ the /etc/hosts.allow เท่านั้น เมื่อมีการ scan ระบบจะแสดงรายชื่อพอร์ตที่เปิดอยู่ และเมื่อผู้โจมตีพยายามเจาะเข้ามาทางพอร์ตที่เปิดอยู่นั้น TCP Wrapper ก็จะปฏิเสธการเชื่อมต่อที่เข้ามาที่ไม่ได้มาจาก host หรือ domain ที่ได้รับอนุญาต แต่ข้อเสียของ TCP Wrapper คือไม่สามารถตรวจสอบได้ครอบคลุมทุกบริการ อย่างเช่น http และ smtp ถ้าทำการตั้งค่าไม่เหมาะสมจะทำให้เสี่ยงต่อการถูกบุกรุกได้ TCP Wrappers ไม่มีจุดอ่อนในเรื่องของ IP spoofing เพราะเมื่อมีการร้องขอเข้ามาTCP Wrapper จะทำ reverse DNS lookup สำหรับ IP address ที่ร้องขอเข้ามา ถ้าค้นพบว่ามีชื่อ domain ตรงกับ IP ที่ร้องขอเข้ามา TCP Wrapper ก็จะอนุญาตการเชื่อมต่อนั้น แต่ถ้าไม่พบ domain ที่ตรงกับ IP TCP Wrapper ก็จะพิจารณาว่าเป็น host ที่ไม่ได้รับอนุญาตและจะไม่ให้ทำการเชื่อมต่อเข้ามา

และวิธีสุดท้ายในการจำกัดจำนวนข้อมูลที่จะให้แก่ port scans คือ การใช้ PortSentry ผลิตโดย Psionic สำหรับ PortSentry นั้นจะตรวจจับการเชื่อมต่อที่ร้องขอเข้ามาที่พอร์ตจำนวนหนึ่ง และสามารถตั้งค่าให้ไม่ต้องสนใจการร้องขอเข้ามาได้โดยผู้ดูแลระบบสามารถเลือกว่าจะให้ PortSentry สนใจการเชื่อมต่อเข้ามาที่พอร์ตไหน และจะปฏิเสธการร้องขอไหนบ้าง ผู้ดูแลระบบจะต้องระบุรายการพอร์ตที่ระบบไม่สนับสนุนไว้ PortSentry จะตรวจจับโดยการใช้ TCP Wrapper และใส่ข้อมูลของผู้บุกรุกที่น่าสงสัยไว้ในไฟล์ /etc/hosts.deny PortSentry จะสร้าง default route statement ให้แก่ระบบที่บุกรุก โดยจะทำให้มีการสร้างเส้นทางให้แก่ทุก ๆ packets จากระบบที่ทำการบุกรุกไปยังระบบอื่นหรือไม่ก็ระบบที่ไม่ได้เปิดอยู่ ทำให้ผลลัพธ์ที่ได้ คือ เสมือนว่าเครื่องเป้าหมายไม่มีตัวตนอยู่จริง บนระบบ Linux PortSentry สามารถตรวจจับการ scan ด้วย TCP และ UDP ทุกชนิด ขณะที่ระบบ Solaris สามารถตรวจจับได้เพียงการ scan แบบ TCP Vanilla และ UDP

**บทสรุป**

ทุก ๆ ระบบมีความเสี่ยงต่อการทำ port scanning ทั้งสิ้น การรุกที่ดีที่สุด คือ การรับที่ดี ดังนั้นอย่ายอมรับการติดตั้งระบบปฏิบัติการด้วยค่าที่ตั้งไว้ให้ตั้ง แต่ต้น เพราะค่าเหล่านั้นส่วนใหญ่จะมีการเปิดพอร์ตไว้มากมายเพื่อให้ใช้งานได้สะดวกขึ้น ก่อนที่จะเปิดให้บริการในระบบ จึงควรทำ port scan ระบบคุณเสียก่อน ถ้าพบว่ามีพอร์ตที่ไม่จำเป็นต้องใช้ก็ปิดพอร์ตเหล่านั้น เพราะยิ่งมีการบริการเปิดไว้มากก็ยิ่งทำให้ระบบมีจุดอ่อนมากขึ้นไปด้วย ควรทำการตรวจสอบไฟล์ /etc/inetd.conf, /etc/init.d และไฟล์ run control บนระบบของคุณอย่างสม่ำเสมอเพื่อค้นหาบริการที่ไม่จำเป็น ถ้าระบบคุณถูกบุกรุก ผู้โจมตีจะพยายามเปิดพอร์ตบนระบบของคุณเพิ่มขึ้นเพื่อที่จะสามารถเจาะเข้ามาที่จุดอ่อนของพอร์ตได้ง่ายขึ้น ดังนั้นยิ่งผู้ดูแลระบบมีความรอบคอบมากเท่าไร ก็ยิ่งทำให้ระบบมีความต้านทานต่อการเจาะเข้ามามากขึ้นและมีโอกาสถูกบุกรุกน้อยลงเท่านั้น

**เอกสารอ้างอิง**


1. Anonymous. Maximum Security, Second Edition. Indianapolis: SAMS, 1998. 177 – 180.

2. McClure, Stuart; Scambray, Joel; Kurtz, George. Hacking Exposed, Network Security Secrets & Solutions. Berekley: Osborne/McGraw Hill, 1999. 38 – 51.

3. Fyodor. "The Art of Port Scanning." September 01, 1997. URL: http://www.insecure.org/nmap/nmap_doc.html. (September 25, 2001).

4. Psionic Software, Inc. URL: http://www.psionic.com/abacus/portsentry. (September 25, 2001).

5. Venema, Wietse. "TCP Wrappers 7.6 BLURB." March 21, 1997. URL: ftp://ftp.porcupine.org/pub/security/tcp_wrappers_7.6.BLURB. (September 25, 2001).


ที่มา: http://thaicert.nectec.or.th/paper/auditing/portscan.php