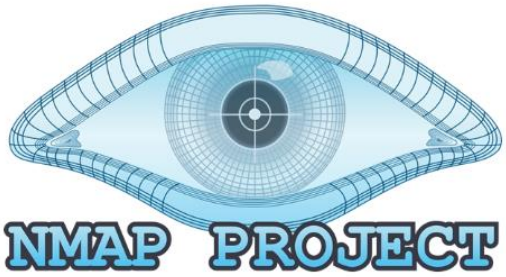
10 สุดยอดเครื่องมือที่ใช้บุกรุกเครือข่าย 2016 : Top 10 Hacker Tools 2016

ผู้ช่วยศาสตราจารย์ ดร.กิตติพงษ์ สุวรรณราช : เขียน
Asst. Prof. Dr. KittipongSuwannaraj
ECA , MTCNA, MTCUME, MTCTCE, RHCT
kitti@psru.ac.th

ถ้าเราพูดถึง “10 สุดยอด เครื่องมือในการบุกรุก” หรือที่เหล่าบรรดา Hacker หรือ วิศวกรด้านความปลอดภัย (Security Engineers) มักจะใช้ในการทดสอบระบบ หรือเจาะระบบนั้น เมื่อเร็วๆ นี้มีการเปิดเผยโดยเว็บไซต์ www.concise-courses.com ซึ่งได้ทำการรวบรวมสุดยอดเครื่องมือที่ใช้ในการเจาะระบบไว้ให้ ซึ่งเครื่องมือเหล่านี้ผมเองก็ได้เคยลองใช้งานหลาย ๆ ตัว ต้องบอกว่ามันสามารถให้รายละเอียดหรือข้อมูลในการเข้าบุกรุกเครือข่ายได้เป็นอย่างดี และแน่นอนครับ นอกจากจะเป็นเครื่องมือในการบุกรุกเครือข่ายที่เหล่า Hacker ใช้งานกันแล้ว เรา ๆ ในฐานะที่เป็นผู้ดูแลระบบหรือเว็บไซต์ของหน่วยงานก็ควรที่จะศึกษาหรือลองใช้เครื่องมือเหล่านี้ไว้บ้าง เพื่อตรวจสอบว่า Server ที่เรากำลังดูแลอยู่นั้นมีจุดอ่อนตรงไหนบ้าง จะได้แก้ไขได้อย่างถูกทาง

เรามาทำความรู้จักกับ 10 สุดยอดเครื่องมือในการ Hacking ระบบกันเลยว่า มีเครื่องมือใดบ้าง และมีความสามารถอย่างไร

1. **NMAP Project** เป็นเครื่องมือที่ใช้ในการ Scan ports และ Map Networks หรือที่เราเรียกว่าเป็น Network Mapper ซึ่งมีชื่อเสียงมากในกลุ่มของ Open Source เครื่องมือนี้รองรับการทำงานบนหลาย ๆ platform ไม่ว่าจะเป็น Linux , FreeBSD , Ms Windows, Mac OS X ด้วย หน้าที่หลัก ๆ หรือความสามารถที่โดดเด่นคือ การ Scan ports และการให้ข้อมูลเกี่ยวกับ Map Networks เราสามารถศึกษาหรือหารายละเอียดเพิ่มเติมได้จาก https://nmap.org



2. **Metasploit Penetration Testing Software** เป็นเครื่องมือที่อยู่ในกลุ่ม Software ที่เรียกว่า Penetration Testing Software หรือที่เรียกว่า ซอฟต์แวร์ที่ใช้ในการทดสอบการเจาะระบบ ซึ่งแน่นอนครับ ก็เป็นประโยชน์สำหรับเราและ Hacker ด้วยเช่นเดียวกันที่จะใช้เครื่องมือนี้ในการตรวจสอบระบบเป้าหมายว่ามีจุดอ่อนอย่างไร มีช่องโหว่ด้านความปลอดภัยอย่างไร (Security vulnerabilities) โดยส่วนมากแล้วผู้ดูแลระบบมือใหม่มักจะไม่เคยลองใช้ Software ด้านนี้ในการตรวจทานระบบตัวเอง ซึ่งก็เท่ากับทำให้ระบบของเรามีความเสี่ยงสูงนั้นเอง เราสามารถดูรายละเอียดเพิ่มเติมได้จาก https://www.metasploit.com/

10 สุดยอดเครื่องมือที่ใช้บุกรุกเครือข่าย 2016 : Top 10 Hacker Tools 2016

3. **John The Ripper** เป็นเครื่องมือประเภท Password Cracking Tool หลายท่านก็เรียกโปรแกรมนี้ว่า “John” หรือ JTR เครื่องมือนี้มีชื่อเสียงมากในการ Crack password และจะสามารถถอดรหัสได้เร็วมาก หากรหัสผ่าน (Password) นั้น กำหนดตาม Dictionary เช่น คำว่า apple , dog , bird อะไรประมาณนี้ ซึ่งการกำหนดรหัสผ่านที่ดี เราควรหลีกเลี่ยงการตั้งรหัสผ่านที่อยู่ใน Dictionary ไม่อย่างนั้นเครื่องมือนี้จะถอดรหัสผ่านของคุณได้อย่างรวดเร็ว การตั้งรหัสผ่านที่ดีนั้น ควรเป็นตัวอักษรที่ประกอบด้วยตัวอักษรตัวภาษาอังกฤษใหญ่ เล็ก เครื่องหมายพิเศษ และความมีความยากมากพอสมควร เช่น มีความยาวมากกว่า 12 ตัวอักษรเป็นต้น โปรแกรม John นี้จะต้องทำงานร่วมกันไฟล์ที่ต้องการถอดรหัสที่อยู่ในลักษณะการทำงานแบบ Offline และเราสามารถนำโปรแกรม John มาใช้งานได้ฟรีอีกด้วย เราสามารถอ่านรายละเอียดได้จาก http://www.openwall.com/john/

4. **THC Hydra** หรือเราจะมักเรียกสั้นๆ ว่า Hydra โปรแกรมนี้เรียกว่าเป็น Password Cracking Tool อยู่ในกลุ่มเดียวกันกับ John The Ripper ครับ มีความสามารถในการการถอดรหัสแบบ Online และนิยมใช้ในการทำ brute-force attacks ไม่ว่าคุณจะใช้ Server จำพวก POP3, IMAP, Databases , LDAP , SMB , VNC, SSH เจ้า Hydra ก็มักจะเป็นเครื่องมือหนึ่งที่เหล่าบรรดา Hacker นิยมใช้งานอย่างมาก เราสามารถติดตามอ่านรายละเอียดเพิ่มเติมได้จาก http://sectools.org/tool/hydra/

5. **OWASP Zed** เราเรียกสั้นๆ ว่า OWASP เครื่องมือนี้เราเรียกว่าเป็น Web Vulnerability Scanner ตัวหนึ่งที่ได้รับความนิยมมากพอสมควร เนื่องจากมี Community เกี่ยวกับ OWASP Zed ก็จำนวนหนึ่ง ซึ่งเจ้า OWASP Zed นี้ถือว่าใช้ในงาน Penetration Tester ได้ดี เราสามารถติดตามอ่านรายละเอียดได้ที่ www.owasp.org

10 สุดยอดเครื่องมือที่ใช้บุกรุกเครือข่าย 2016 : Top 10 Hacker Tools 2016

6. **Wireshark** เป็นเครื่องมือประเภท Web Vulnerability Scanners ที่ได้รับความนิยมมากเครื่องมือหนึ่งที่ Hacker หรือ Softeware Engineers นิยมใช้เพื่อ captures data packet ที่อยู่ใน Network ที่ทำงานแบบ Real time และสามารถแสดงผลได้ทันที เครื่องมือนี้สามารถที่จะ filter เฉพาะข้อมูลที่เรากำลังสนใจได้ โดยการแบ่งออกเป็นสีต่างๆ เพื่อให้ง่ายแก่การตรวจดูข้อมูลที่เราสนใจ ปัจจุบันมีผู้สนใจ Wireshark เป็นจำนวนมาก มีการทำสื่อเกี่ยวกับ Wireshark และวิดีโอการเรียนรู้ออกมามาก พร้อมมีการสอบ Certification อีกด้วย เราสามารถดูรายละเอียดเพิ่มเติมได้จาก www.wireshark.org

7. **Aircrack-ng** เป็นเครื่องมือที่สามารถใช้งานได้ฟรี มีหน้าที่เป็น Password Cracking Tool ที่ทำงานผ่านระบบ WiFi ตามมาตรฐาน 802.11 ทั้ง WEP และ WPA keys ซึ่งจะทำงานได้ดีใน Monitor mode และ FMS Attacks หรือที่บางครั้งเรียกว่า Korek attacks (PTW attacks) เครื่องมือนี้มีความสามารถในการ crack WEP ได้ในไม่กี่นาที และรวมถึ WPA/WPA2 ด้วย ซึ่งนับเป็นเครื่องมือที่มีการพูดถึงมากที่สุดในประเภทเครื่องมือที่เป็น WiFi Cracking เราสามารถอ่านรายละเอียดเพิ่มเติมได้จาก https://www.**aircrack-ng**.org/

8. **Maltego** เป็นเครื่องมือที่สามารถใช้งานได้ฟรี และมีแบบจ่ายเงินเพิ่ม เครื่องมือนี้มีความแตกต่างจากเครื่องมือประเภทอื่นๆ คือ มันจะทำหน้าที่เป็น Digital forensics โดยอาศัยหลักการของ Data mining ในการติดตามแกะรอยข้อมูลที่เรากำลังสนใจ ซึ่งสามารถวิเคราะห์ข้อมูลได้แบบ Real time และทำงานได้บนหลายๆ platform เพื่อให้เราสามารถเรียกดูข้อมูลได้ง่ายและสะดวก เราสามารถติดตามรายละเอียดได้จาก www.paterva.com/web7/buy/maltego-clients/maltego-ce.php

10 สุดยอดเครื่องมือที่ใช้บุกรุกเครือข่าย 2016 : Top 10 Hacker Tools 2016

9. **Cain and Abel Hacking Tool** เครื่องมือนี้ทำหน้าที่เป็น Password Cracker/ Password Hacking ที่มีการพูดถึงมากพอสมควร เราจะรู้จักในชื่อเรียกสั้นๆ ว่า “Cain” นั้นเอง หลาย ๆ คนที่ฝึกหรือเรียนรู้เกี่ยวกับการ Crack หรือ Hack ก็จะใช้เครื่องมือนี้ในการทำ Lab หรือทำเป็น Hacking Tutorials เจ้า Cain นี้ก็ถูกนำมาใช้งานในหลาย ๆ วัตถุประสงค์ ไม่ว่าจะเป็นการ crack password หรือการ Password Hashing ร่วมกับ dictionary attacks , brute force หรือ rainbow table attacks เป็นต้น เราสามารถอ่านข้อมูลเพิ่มเติมได้จากเว็บไซต์ sectools.org/tool/cain

10. **Nikto Website Vulnerability Scanner** เครื่องมือนี้สามารถใช้งานได้ฟรี ทำหน้าที่เป็น Website Vulnerability Scanner Hacking Tool ที่ผู้ทดสอบระบบใช้งานกัน โดยโปรแกรม Nikto นี้ได้รับการสนับสนุนจาก Netsparker อีกทีหนึ่ง โปรแกรม Nikto นี้เป็น Open source software ที่ทำงานแบบ web server scanner ซึ่งจะทำการตรวจสอบ Web Server และช่องโหว่ต่าง ๆ โดยจะทำการตรวจสอบการ config server ในหัวข้อต่าง ๆ จากหลายๆ index files และรวมถึง HTTP Server options ต่าง ๆ ที่ได้มีการติดตั้งไว้แล้วบนเซิร์ฟเวอร์นั้น เราสามารถติดตามอ่านรายละเอียดเพิ่มเติมได้จาก https://cirt.net/nikto2

เมื่อเราทราบถึงเครื่องมือต่างๆ ที่ Hacker ใช้ในการบุกรุกเครือข่ายแล้ว เราก็ควรที่จะศึกษา หรือนำมาทดสอบและวัดกับเครื่องเซิร์ฟเวอร์ของเราว่า ผ่านการทดสอบหรือไม่ หากโปรแกรมแจ้งว่ามีช่องโหว่ เราก็ควรเร่งมือหาทางแก้ไขก่อนที่ Hacker จะ Scan พบช่องโหว่ดังกล่าวแล้ว เล่นงานเราในเวลาต่อไป

ท้ายนี้หวังเป็นอย่างยิ่งว่าความรู้ที่ได้จากบทความนี้ คงจะเป็นประโยชน์ต่อผู้อ่านทุกท่านครับ

10 สุดยอดเครื่องมือที่ใช้บุกรุกเครือข่าย 2016 : Top 10 Hacker Tools 2016

แหล่งสืบค้นเพิ่มเติม :

https://www.concise-courses.com/hacking-tools/top-ten/

https://nmap.org

https://www.metasploit.com/

http://www.openwall.com/john/

http://sectools.org/tool/hydra/

www.owasp.org

www.wireshark.org

https://www.**aircrack-ng**.org/

www.paterva.com/web7/buy/maltego-clients/maltego-ce.php

sectools.org/tool/cain

https://cirt.net/nikto2

Article Number : 201610300712