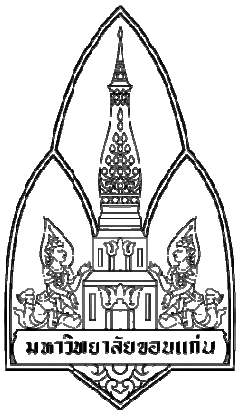


รายงาน เรื่อง Snort

สมาชิกกลุ่ม 8

8.1 น.ส.ธันย์ชนก คุณวัฒน์บัณฑิต 583020665-0

8.1 น.ส.นวพร กิ่งสาร 583020666-8

8.2 น.ส.วิลาสินี โพธิ์เกตุ 583020678-1

8.2 น.ส.กวิสรา อังมีพิษ 583021364-9

8.3 น.ส.พนิดา แพงมา 583021385-1

8.3 น.ส.ภัทรกันย์ เคนคำภา 583021391-6

เสนอ

ผศ.ดร.จักรชัย โสอินทร์

รายงานเล่มนี้เป็นส่วนหนึ่งของรายวิชา 322222 NETWORK I

เครือข่าย 1Section 4

ภาคการศึกษาที่2 ปีการศึกษาที่ 2560

คณะวิทยาศาสตร์ มหาวิทยาลัยขอนแก่น

ความเป็นมาและความสำคัญ

ถ้าจะกล่าวถึงยุคปัจจุบัน น่าจะกล่าวดาว่าเป็นยุคแห่งเทคโนโลยี ไม่ว่าจะเป็นการพัฒนาหรือการแข่งขันกันอย่างรุนแรงทางด้านไอที องค์กรใดที่มีข้อมูลมากกว่า องค์กรนั้นย่อมมีโอกาสได้มากกว่า จึงถือได้ว่าข้อมูลสารสนเทศเหล่านี้ เทียบได้กับทองคำทีมีของแต่ละองค์กร ในขณะเดียวกันอุปกรณ์ทางด้านไอทีก็ได้เข้ามามีส่วนร่วมในชีวิตประจำวันของเราอย่างมาก จึงปฏิเสธไม่ได้ว่าข้อมูลสารสนเทศเป็นสิ่งที่จำเป็นในอุปกรณ์ไอทีด้วย เพราะข้อมูลเหล่านี้จะถูกบันทึกอยู่ในรูปแบบต่างๆ ทางด้านไอที เพื่อความสะดวกในการเก็บรักษาและการนำไปใช้งาน ดังนั้นข้อมูลสารสนเทศที่ถือเป็นของมีค่า จึงเป็นที่ต้องการขององค์กรที่เป็นคู่แข่งหรือองค์กรต่างๆที่มีส่วนเกี่ยวข้อง ทำให้ข้อมูลสารสนเทศนั้นเกิดความไม่ปลอดภัย จำเป็นอย่างยิ่งที่จะต้องมีการป้องกันหรือรักษาความปลอดภัย ไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้าใช้งานข้อมูลเหล่านั้น สามารถที่จะเข้าถึงและนำข้อมูลนำไปใช้ได้ จึงได้มีการติดตั้งระบบรักษาความปลอดภัยขึ้นเพื่อ เอาไว้ใช้ในการดูแลและปกป้องข้อมูลสารสนเทศต่างๆ

ปัจจุบันองค์กรส่วนมากมีการนำเอาระบบการรักษาความปลอดภัยให้กับข้อมูลและสารสนเทศแบบต่างๆ ไม่ว่าจะเป็นการเข้ารหัสข้อมูล โปรแกรมป้องกันไวรัส หรือการติดตั้งอุปกรณ์ทางด้านฮาร์ดแวร์(Hardware) เช่น ไฟร์วอล์(Firewall) หรือจะเป็นระบบตรวจจับการบุกรุกที่มีให้เลือกอยู่มากมายในขณะนี้ และถ้ากล่าวถึงระบบตรวจจับการบุกรุก ระบบที่หลายๆคนรู้จักก็คือ ระบบตรวจจับการบุกรุก Tripwire , Nessus , Snort เนื่องจากทั้งสามนี้ต่างก็เป็นระบบที่มีคนรู้จักและใช้งานอย่างแพร่หลาย สาเหตุที่ทำให้สามกลายเป็นที่นิยมก็เพราะเป็น โอเพ่นซอร์ส (Open Source) สามารถนำไปใช้งานได้ฟรี ไม่ต้องเสียค่าใช้จ่ายใดๆ และมีประสิทธิภาพที่ไม่ได้ด้อยไปกว่าระบบตรวจจับการบุกรุกที่เป็นแบบเชิงธุรกิจ

เมื่อกล่าวถึง Snort อย่างที่ทราบกันดีว่า Snort เป็นซอฟต์แวร์ที่อยู่ในกลุ่ม Network Intrusion Detection System (NIDS) ซึ่งทำหน้าที่ตรวจหาการบบุกรุกภายในเครือข่าย ด้วยการดักจับแพ็กเก็ตข้อมูลที่ส่งผ่านในเครือข่ายคอมพิวเตอร์ ซอฟต์แวร์นี้มีข้อดีคือทำให้ผู้ใช้ได้ทราบถึงความพยายามในการโจมตี โปรแกรมนี้มีประโยชน์ในการแจ้งเตือน เมื่อมีความพยายามในการบุกรุกเกิดขึ้นเพื่อจะได้หาทางแก้ไขและป้องกันต่อไป โปรแกรม Snort ซึ่งในการติดตั้งจำเป็นที่จะต้องอาศัยความรู้ความชำนาญในการติดตั้งรวมไปถึงการปรับแต่งค่า และการใช้งาน

Snort นั้นจะอยู่ในรูปแบบของ Command line จำเป็นที่จะต้องพิมพ์คำสั่งลงไปเอง เพราะฉะนั้น ผู้ใช้งานจำเป็นต้องมีความรู้ ความชำนาญ

ผู้จัดทำจึงได้ทำการศึกษา Snort ซึ่งเป็นซอฟท์แวร์สำหรับตรวจจับผู้บุกรุกในระบบเครือข่าย หรือที่เรียกว่า Network Intrusion Detection System (NIDS) ซึ่งโปรแกรม Snort มีข้อดีคือทำให้ทราบถึงความพยายามในการโจมตี โดยจะทำการแจ้งเตือนเมื่อมีความพยายามในการบุกรุกเกิดขึ้น ผู้จัดทำมีความต้องการทดสอบการทำงานของ snort โดยทำการติดตั้งโปรแกรมสำหรับแฮ็คข้อมูลแล้วโจมตีไปที่คอมพิวเตอร์ที่ติดตั้ง snort เพื่อศึกษาการตรวจจับผู้บุกรุกของโปรแกรม

วัตถุประสงค์

- เพื่อศึกษาการทำงานของโปรแกรม Snort
- ติดตั้งโปรแกรม Snort เพื่อตรวจกับการบุกรุกในระบบเครือข่าย

ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

ระบบตรวจหาการบุกรุก (Intrusion Detection Systems) มีงานวิจัยอย่างหลากหลายเพื่อพัฒนาวิธีการวิเคราะห์รูปแบบพฤติกรรมจากแพ็กเก็ตข้อมูลที่ส่งผ่านระหว่างเครื่องคอมพิวเตอร์ที่เชื่อมโยงต่อภายในเครือข่ายค้นหาสิ่งที่ผิดปรกติ (Anomaly) แล้วนำเข้าสู้กระบวนการทำนายเพื่อตัดสินว่าเป็นเหตุการณ์บุกรุกจริงแล้วแจ้งเตือน (Alert) ให้ผู้รับผิดชอบเครือข่ายทราบเพื่อดำเนินการป้องกันและแก้ไข

ดร. ธีรเกียรติ์ เกิดเจริญ วิจัยเรื่อง ระบบเครือข่าย และ ความปลอดภัย มีวัตถุประสงค์เพื่อเพิ่มความรู้ความเข้าใจในเรื่องของความปลอดภัยในการใช้ระบบเครือข่าย โดยผู้ใช้จะต้องรู้จักกับการโจมตีที่หลลากหลายรูปแบบ การรักษาความปลอดภัยจากการโจมตี โดยผู้วิจัยได้ใช้ความรู้ทางด้านเทคโนโลยีสารสนเทศ ในการพัฒนาการรักษาความปลอดภัยบนเครือข่ายให้ทำงานได้อย่างมีประสิทธิภาพสูง มีระบบรักษาความปลอดภัยที่ดีมีความน่าเชื่อถือสูง และสามารถที่นำไปพัฒนาต่อไป

ดร.โกเมน พิบูลโรจน์ วิจัยเรื่อง เทคนิคการโจมตีแบบ Phishing มีวัตถุประสงค์ เพื่อเพิ่มความรู้ความเข้าใจในเรื่อง การโจมตีในรูปแบบของการปลอมแปลงอี-เมล์ (Email Spoofing) และการทำการสร้างเว็บไซต์ปลอม เพื่อทำการหลอกลวงให้เหยื่อหรือผู้รับอี-เมล์เปิดเผยข้อมูลทางด้านการเงินหรือข้อมูลส่วนบุคคลอื่นๆ อาทิ ข้อมูลของหมายเลยบัตรเครดิต บัญชีผู้ใช้ (Username) และ รหัสผ่าน (Password) หมายเลขบัตรประจำตัวประชาชน หรือข้อมูลส่วนบุคคลๆ

โปรแกรม Snort IDS

ความหมายของโปรแกรม Snort

โปรแกรม Snort เป็นโปรแกรมตรวจจับการบุกรุกที่มีขนาดเล็ก มีการใช้ทรัพยากรน้อยทำให้ไม่สิ้นเปลือง โปรแกรมตรวจจับการบุกรุก Snort จัดเป็นระบบตรวจจับการบุกรุกบนเครือข่าย ที่สามารถตรวจจับได้อย่างรวดเร็ว มีการทำงานเป็นแบบ Real Time ตรวจจับการบุกรุกด้วยวิธี Misuse Detection มีภาษาที่ใช้ในการเขียนรูปแบบการโจมตี (Rules) ที่สามารถเข้าใจได้ง่ายและมีความยืดหยุ่น

และเนื่องจาก นี้ยังเป็นโอเพนซอส (Open Source) ตามข้อตกลงของ General Public License หรือ GNU จึงสามารถนำไปใช้งานได้โดยไม่ต้องเสียค่าใช้จ่ายใดๆ ด้วยคุณสมบัติต่างๆ เหล่านี้นี่เองทำให้ระบบตรวจจับการบุกรุก Snort จึงกลายเป็นที่นิยม มีการนำไปใช้งานกันอย่างแพร่หลาย

โครงสร้างของระบบตรวจจับการบุกรุก Snort สามารถแบ่งได้เป็น 3 ส่วนด้วยกันคือ

1. ส่วนที่ใช้ในการถอดรหัสข้อมูลจากแพ็คเกต (Packet Decoder)

2. ส่วนที่ใช้ในการตรวจสอบหาการบุกรุก (Detection Engine)

3. ส่วนที่ทำการบันทึกข้อมูลและแจ้งเตือน (Logging/Alerting Subsystem)

หลักการทำงานของ Snort

ระบบตรวจจับการบุกรุก Snort ระบบตรวจจับการบุกรุกนี้มีลักษณะของการทำงานอยู่ 4 ประเภทด้วยกัน คือ

(1) Sniffer Mode – ใช้ในการดักจับข้อมูลบนเครือข่ายเพื่อใช้ในการวิเคราะห์พฤติกรรมการใช้งานของผู้ใช้ในระบบ

(2) Packet Locker Mode – หลักการทำงานคล้ายคลึงกับ Sniffer Mode แต่จะทำการเก็บข้อมูลไว้ใน Database เพื่อใช้ในการวิเคราะห์ในภายหลัง

(3) NIDS Mode (Network Intrusion Detection System Mode) – มีหลักการทำงานคือทำการวิเคราะห์ข้อมูลที่ไหลผ่านระบบ Network แบบ Real Time โดยเทียบกับเงื่อนไข (Rules) เพื่อใช้วิเคราะห์ข้อมูลเหล่านั้นว่าเป็นอันตรายต่อระบบหรือไม่

(4) Inline Mode – เป็น Mode ที่ทำหน้าที่เป็น IPS (Intrusion Protection System) ซึ่งสามารถวิเคราะห์ข้อมูลที่ไหลผ่านแบบ Real Time โดยเทียบกับเงื่อนไขแบบใหม่ (New Rules) เพื่อใช้ในการตัดสินใจและกรองข้อมูลที่ต้องสงสัยว่าจะเป็นอันตรายต่อระบบ

การทำงานของโปรแกรม Snort

ตรวจจับการบุกรุก Snort จะต้องมีการสั่งงานผ่านทางคอมมานไลน์ (Command line) จึงจำเป็นที่จะต้องทำความรู้จักกับคำสั่งแต่ละคำสั่งก่อน และต่อไปนี้คือ คำสั่งบางคำสั่งที่ใช้ในการสั่งงานระบบตรวจจับการบุกรุก Snort

1. – A ตั้งค่าให้มีการแจ้งเตือน

2. – b เก็บบันทึกข้อมูลแพ็คเกตลงในรูปแบบของ tcpdump

3. – c สั่งเปิดใช้รูปแบบของการโจมตี

4. – C ให้ทำการแสดงค่าที่เป็นข้อมูลตัวหนังสือ

5. – d แสดงผลข้อมูลของแอพพลิเคชั่นเลเยอร์

6. – e แสดงเฮดเดอร์ (Header) ของเลเยอร์ 2

7. – E บันทึกการแจ้งเตือนลงใน NT Eventlog

8. – G ใช้ระบุอีเว้นท์ (Event)

9. – h ทำการตั้งค่าโฮล์มเน็ทเวิร์ค (Home Network)

10. – i เลือกอินเตอร์เฟสที่จะใช้

11. – I สั่งให้เพิ่มชื่อของอินเตอร์เฟสลงในเอาท์พุต (Output)

12. – k สั่งให้ทำงานในโหมด Checksum

13. – K สั่งให้ทำงานในโหมด Logging

14. – l ให้ทำการบันทึกลงในไดเร็กทอรี่ (Directory) นี้

15. – L ให้ทำการบันทึกลงไฟล์ tcpdump นี้

16. – n ออกหลังจากได้รับแพ็คเกต (Packet)

17. – N ปิดการบันทึกแต่ยังทำการแจ้งเตือนำได้อยู่

18. – o เปลี่ยนกฎที่ใช้ในการตรวจจับจากเทสติ้ง (testing) เป็นพาส (pass) แจ้งเตือน (aleart) หรือบันทึก (log)

19. – p ปิดโหมดดักจับข้อมูล

20. – q ปิดโฆษณาและรายงานสถานะ

21. – r อ่านไฟลล์ tcpdump

22. – s ให้ทำการเก็บบันทึกข้อมูลลงใน Syslog

23. – T ให้ทำการทดลองและรายงานผลโดยใช้ค่าที่ปรับแต่ง ณ ปัจจุบัน

24. – V แสดงเวอร์ชัน (Version)

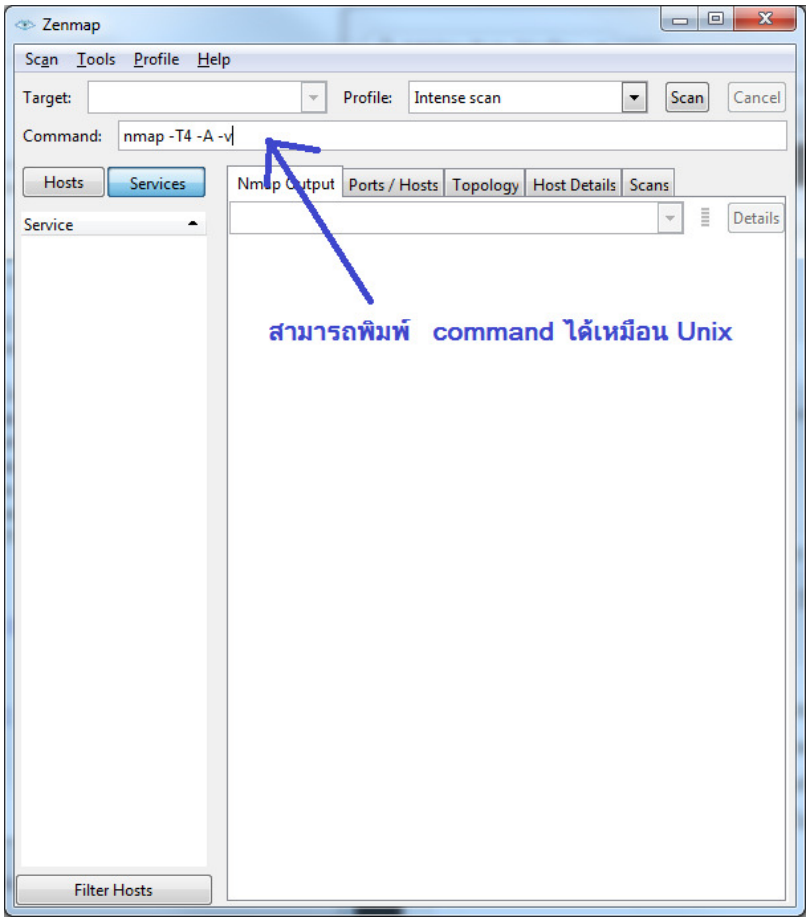
25. – W แสดงอินเตอร์เฟส (Interface) ที่สามารถเลือกใช้งานได้

26. – y เป็นการใส่ปีลงใน Timestamp ในไฟลล์ที่เก็บบันทึกและเก็บการแจ้งเตือน

27. - ? แสดงข้อมูลคำสั่ง

โปรแกรมที่ใช้พัฒนา

Zenamp โปรแกรม NMAP for windows เครื่องมือในการ scan อุปกรณ์ในระบบ network มีอยู่มากมายหลายตัว nmap เป็น ตัวหนึ่งที่ได้ รับความนิยมสูง ซึ่งโดยปกติแล้ว nmap จะรันอยู่บน Unix แต่เนื่องจากความนิยม ผู้พัฒนาได้สร้าง software nmap ที่รันบน OS window 7 ขึ้นไป โดยใช้ ชื่อว่า Zenamp

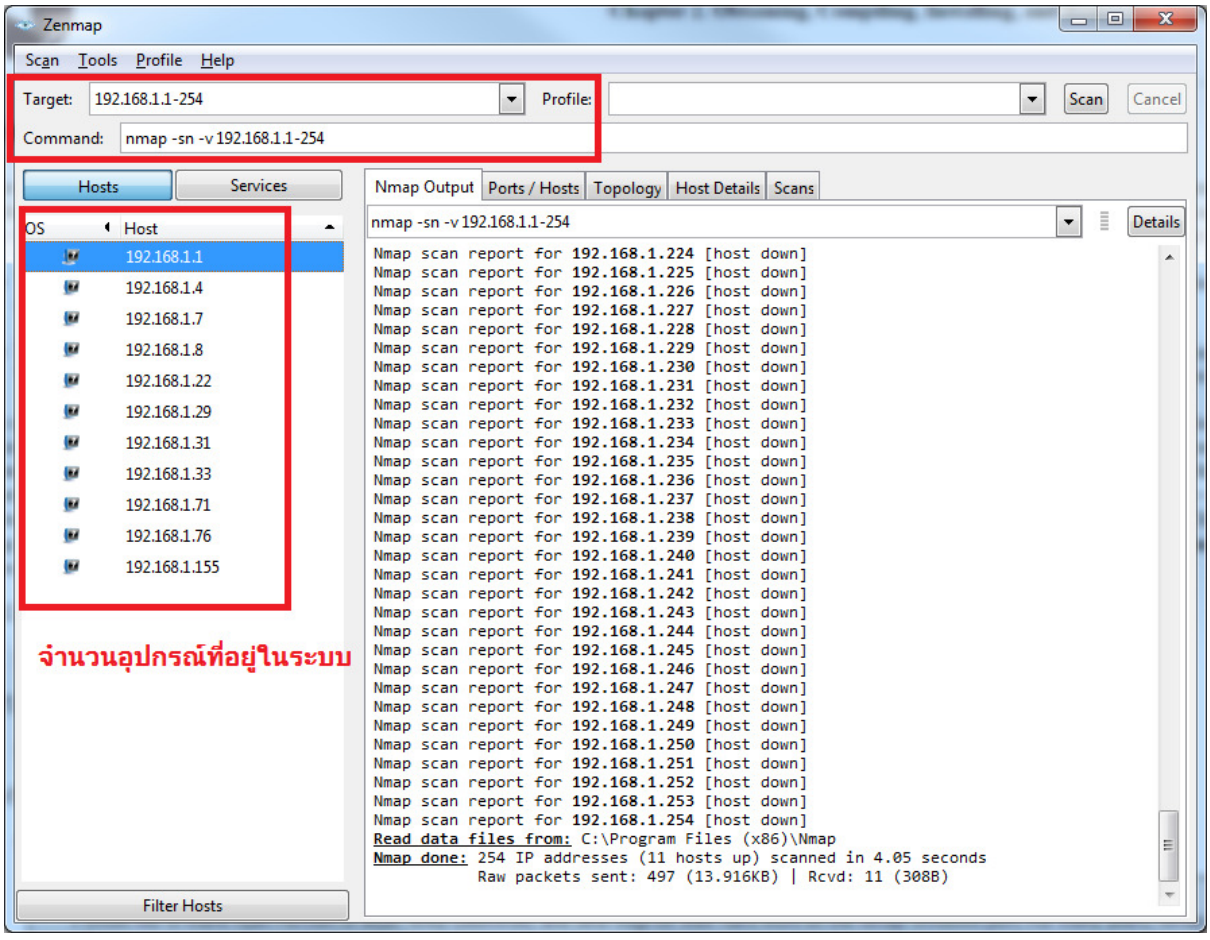


Zenmap เป็นโปรแกรมที่ใช้งานได้เหมือนกับ nmap แต่ยังมีข้อจำกัดบางประการเนื่องจากปัญหาของประสิทธิ์ port ของ window ข้อจำกัดที่ว่าก็คือ

จะไม่สามารถ ทำ loop back 127.0.0.1 หรือ scan ตัวเอง ได้

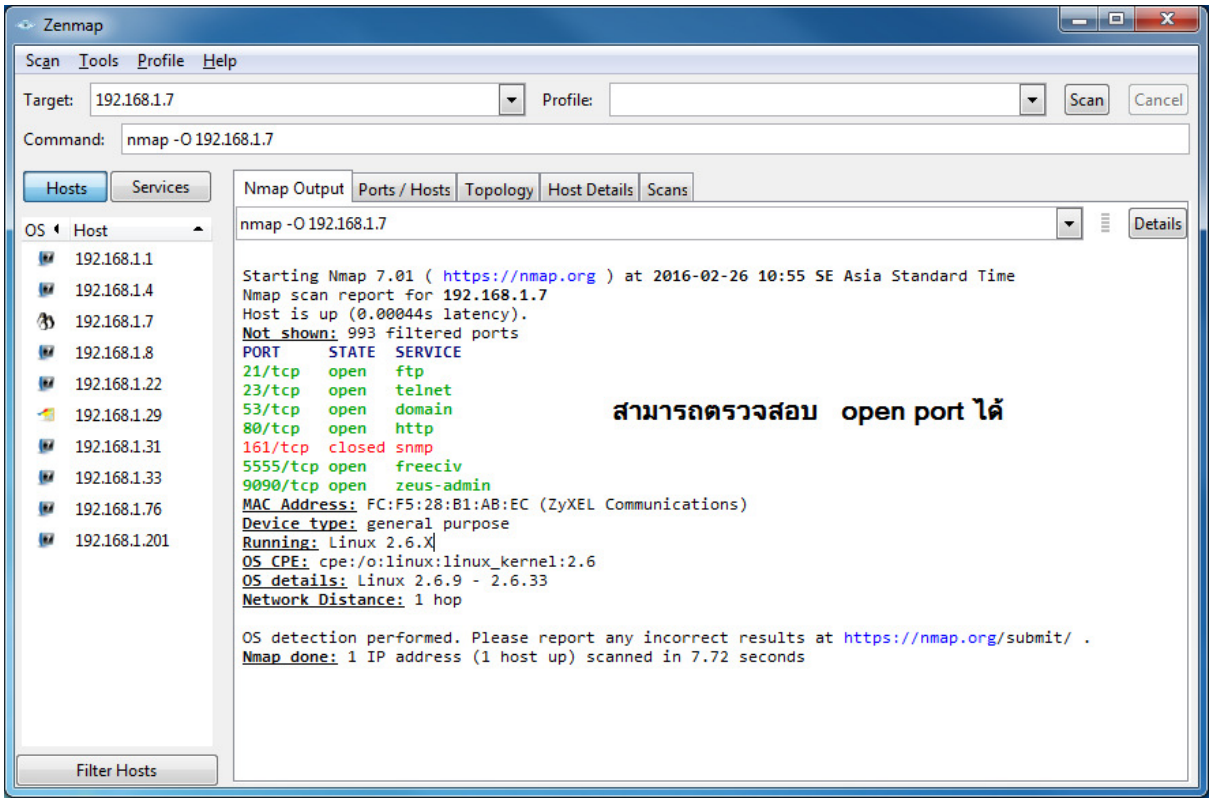
สามารถทำงานได้ดีบน LAN network จนกระทั่งมีการเรียกใช้ -sT -Pn options จะทำให้การทำงาน ผิดพลาดเนื่องจาก Microsoft ตัด raw TCP/IP packet ทิ้งตั้งแต่วินโดว XP sp2 ขึ้นไป

ตัวอย่างการใช้ Zemap ค้นหาอุปกรณ์ใน network ของเราว่ามีใครแอบมาใช้งานหรือไม่ namp -sn -v 192.168.1.1-254 (ทดสอบโดยการ ping scan ตั้งแต่ ip หมายเลข 192.168.1.1 ถึง 192.168.1.254)

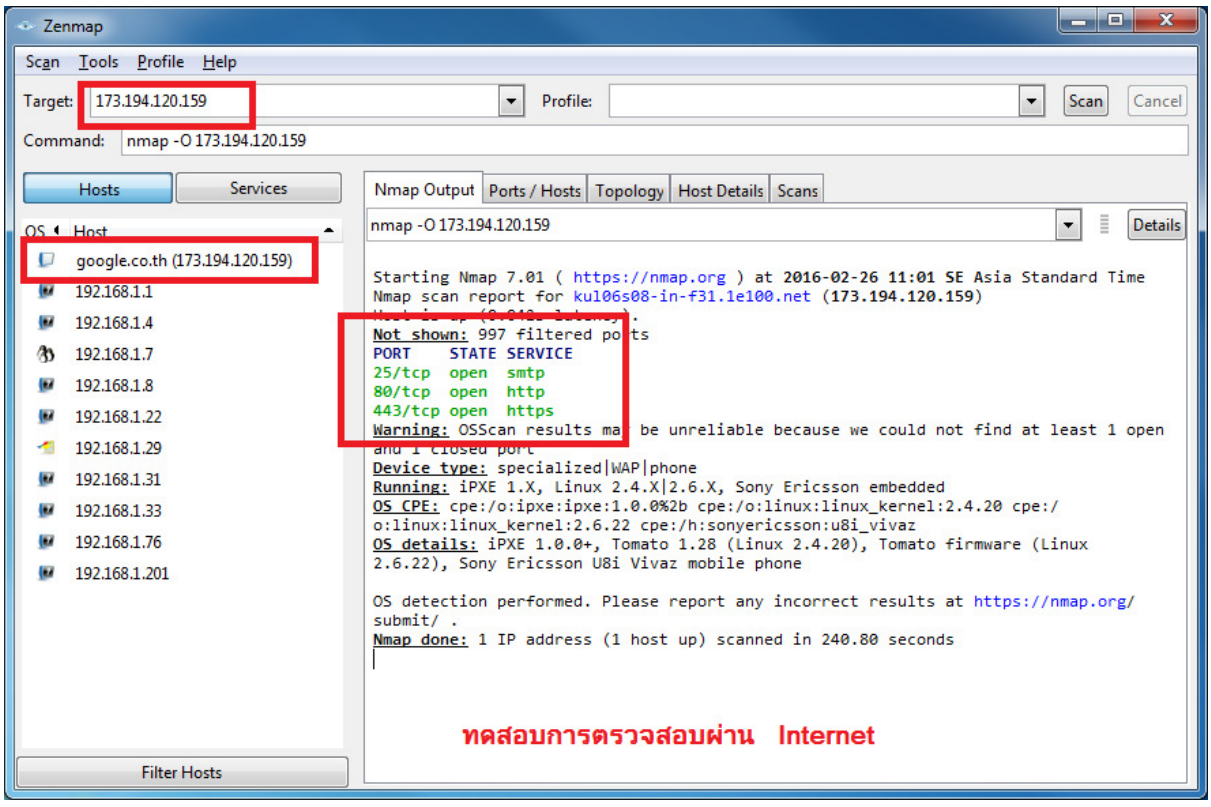


ตัวอย่างการตรวจสอบอุปกรณ์ ภายในวง LAN ค้นหาว่าอุปกรณ์นี้ทำการเปิด port อะไรบ้าง

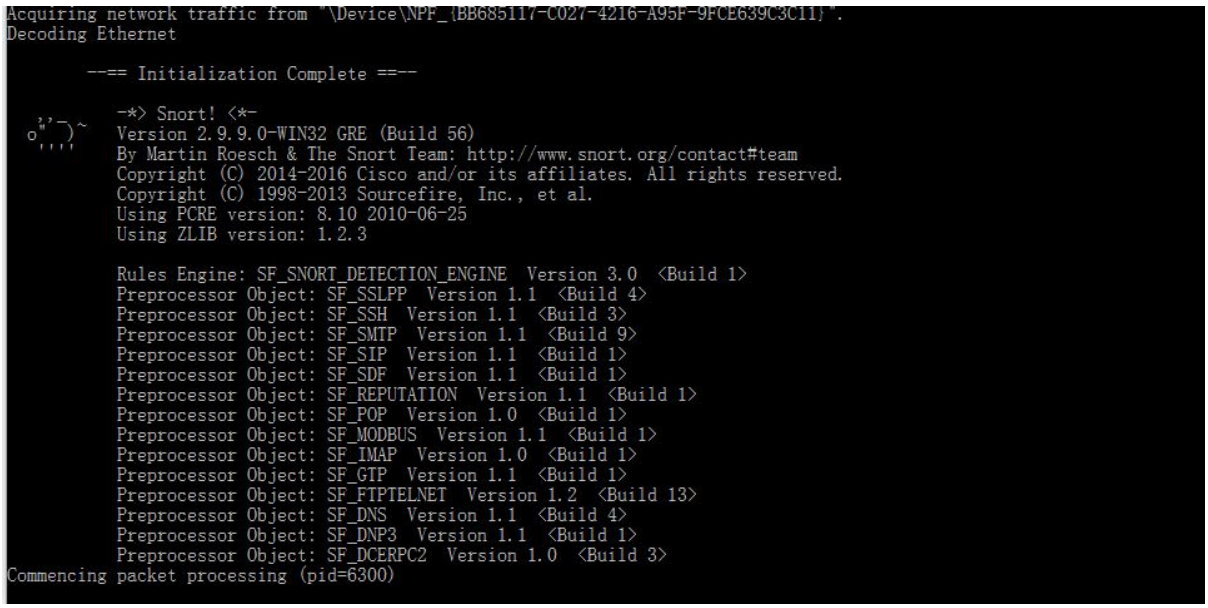
nmap -O 192.168.1.7

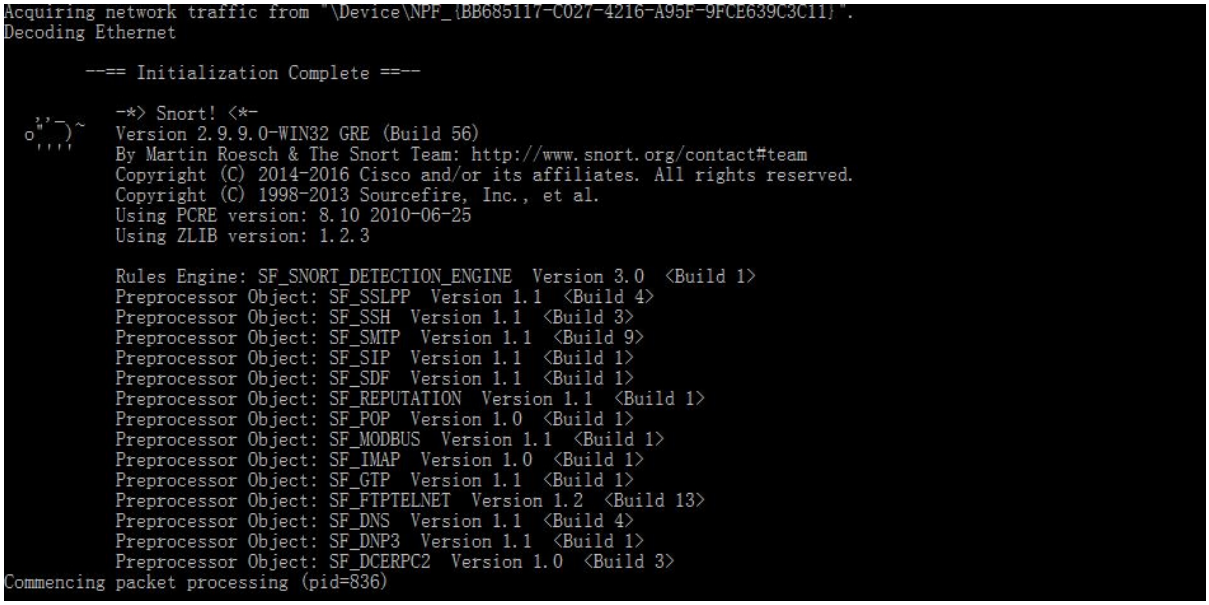


ตรวจสอบอุปกรณ์ ผ่าน internet nmap -O 173.194.120.159 (google)

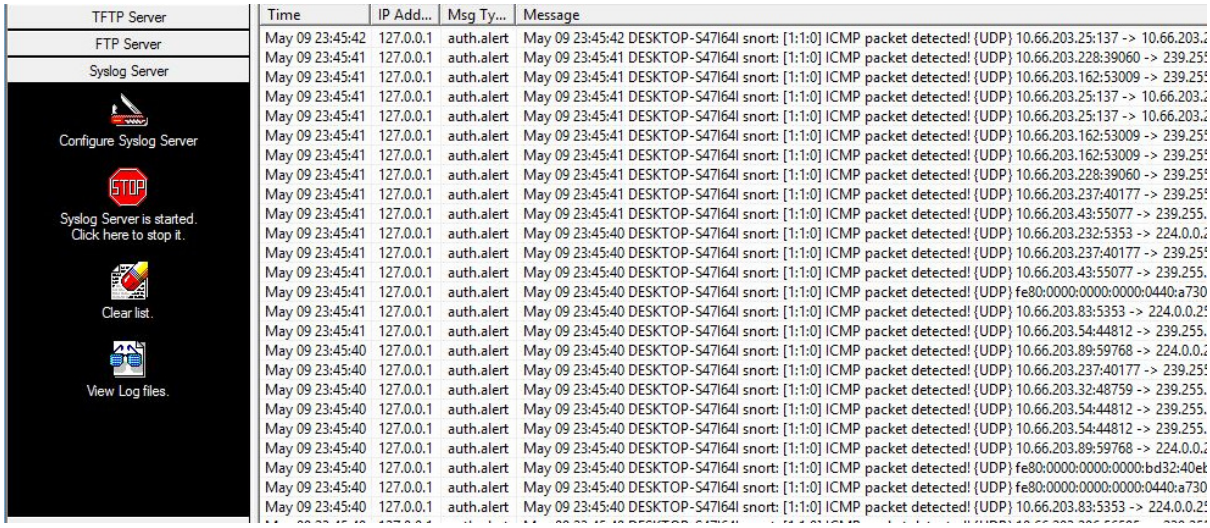


ตัวอย่างแอปพลิเคชั่น





```
  Max concurrent sessions                          : 0
===============================================================================
dcerpc2 Preprocessor Statistics
  Total sessions: 0
===============================================================================
SSL Preprocessor:
   SSL packets decoded: 72
          Client Hello: 6
          Server Hello: 6
           Certificate: 4
           Server Done: 16
   Client Key Exchange: 4
   Server Key Exchange: 4
         Change Cipher: 12
              Finished: 0
    Client Application: 31
    Server Application: 10
                 Alert: 0
  Unrecognized records: 14
  Completed handshakes: 0
       Bad handshakes: 0
     Sessions ignored: 8
    Detection disabled: 5
===============================================================================
SIP Preprocessor Statistics
  Total sessions: 0
===============================================================================
Snort exiting
```




```
Len: 50
+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

05/09-23:49:54.794484 10.66.203.38:5353 -> 224.0.0.251:5353
UDP TTL:255 TOS:0x0 ID:5761 IpLen:20 DgmLen:89
Len: 61
+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

05/09-23:49:54.795128 10.66.203.191:54343 -> 239.255.255.250:1900
UDP TTL:1 TOS:0x0 ID:49077 IpLen:20 DgmLen:153 DF
Len: 125
+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

05/09-23:49:54.896643 10.66.203.31:37521 -> 239.255.255.250:1900
UDP TTL:1 TOS:0x0 ID:51269 IpLen:20 DgmLen:153 DF
Len: 125
+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

*** Caught Int-Signal
05/09-23:49:55.104252 10.66.203.191:54343 -> 239.255.255.250:1900
UDP TTL:1 TOS:0x0 ID:49078 IpLen:20 DgmLen:153 DF
Len: 125
+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

===============================================================================
Run time for packet processing was 10.302000 seconds
Snort processed 179 packets.
Snort ran for 0 days 0 hours 0 minutes 10 seconds
   Pkts/sec:           17
===============================================================================
```

เอกสารอ้างอิง

อติชาติ พานโน. ๒๔๖๐. Snort . (ออนไลน์). แหล่งที่มา :
https://sites.google.com/a/acc.msu.ac.th/54010970425/2. 5 พฤษภาคม 25560.

๒๔๖๐. Zenamp. (ออนไลน์). แหล่งที่มา : http://www.monplern.com/network/zenamp-%E0%B9%82%E0%B8%9B%E0%B8%A3%E0%B9%81%E0%B8%81%E0%B8%A3%E0%B8%A1-nmap-for-windows/. 5 พฤษภาคม 25560.

๒๔๖๐. Snort . (ออนไลน์). แหล่งที่มา : https://nmap.org/. 5 พฤษภาคม 25560.