รายงานเรื่อง DDoS (Distributed Denial of Service)

วิชา 322 376 Information and Communication Technology Security

เสนอ

ผศ.ดร.จักรชัย โสอินทร์

จัดทำโดย

นายรัชชานนท์ ชมภูบุตร	553021012-7
นางสาวศิริรัตน์ สิทธิหาโคตร	553021019-3
นายชัยยุทธ ตั้งขจรศักดิ์	553020980-9
นายปรัชญ์ อรรถวิภานนท์	553020450-8
นายคุณวุฒิ วุฒิสุพงส์	543021199-4

Section 4

สาขาเทคโนโลยีสารสนเทศและการสื่อสาร ภาควิชาวิทยาการคอมพิวเตอร์

คณะวิทยาศาสตร์ มหาวิทยาลัยขอนแก่น

ภาคการศึกษาที่ 1 ปีการศึกษา 2557

คำนำ

รายงาน ฉบับนี้เป็นส่วนหนึ่งของวิชา วิชา 322 376 Information and Communication Technology Security รายงานเล่มนี้จะนำเสนอโปรแกรม Low Orbit Ion Cannon (LOIC) โดยใช้เทคโนโลยีการโจมตี DDoS เพื่อเป็นการโจมตีเครื่องเป้าหมาย ทำให้เครื่องเป้าหมาย มีการทำงานที่ผิดปกติ และวิธีการป้องกันจากเทคโนโลยีการโจมตี DDoS

ในการจัดทำรายงานนำเสนอเนื้อหาข้อมูลในครั้งนี้ ผู้จัดทำขอขอบคุณ ผู้ให้ความรู้ และแนวทางการศึกษา ความช่วยเหลือมาโดยตลอด ผู้จัดทำหวังว่ารายงานฉบับนี้จะให้ความรู้ และเป็นประโยชน์แก่ผู้อ่านทุก ๆ ท่านหากมีข้อผิดพลาดประการใดต้องขออภัยมา ณ ที่นี้ด้วย

คณะ ผู้จัดทำ

สารบัญ

1. วัตถุประสงค์โครงการ

1.1. ใช้โปรแกรม Low Orbit Ion Cannon (LOIC) เพื่อโจมตีเครื่องเป้าหมายให้ได้รับความเสียหาย

1.2. เพื่อเรียนรู้การทำงานของระบบ DDoS

1.3. ศึกษารูปแบบการโจมตีของระบบ DDoS

1.4. ศึกษารูปแบบการป้องกันของระบบ DDoS

2. หลักการและเหตุผล

ปัจจุบันมีการให้บริการข้อมูลผ่านระบบอินเทอร์เน็ตอย่างแพร่หลาย ภายใต้การให้บริการดังกล่าวมีโครงสร้างที่ มีความซับซ้อน ประกอบด้วยอุปกรณ์กระจายและจัดเส้นทาง เพื่อนำข้อมูลจากผู้ใช้บริการไปสู่เครื่องแม่ข่ายที่กระจายตัวอยู่ทั่วโลก และมีการใช้งานระบบเครือข่ายอยู่ตลอดเวลาสลับกันไปตามภูมิภาคและทวีป นอกเหนือจากผู้ใช้บริการและยังมีผู้ใช้บางส่วนที่ ไม่ประสงค์ดีต่อผู้ให้บริการและผู้ใช้ที่ ถูกใช้เป็นเครื่องมือโดยมิได้ตั้งใจ อาจเรียกได้ว่าเป็นอาชญากรรมทางคอมพิวเตอร์ ได้แก่ การลอกลวง การโจมตีเพื่อไม่สามารถให้บริการ เนื่องจากการเชื่อมต่อที มีความเร็วสูงในปัจจุบัน การโจมตีจากจุดเดียวหรือจากผู้ใช้ในบางพื้นที่ อาจไม่ส่งผลกระทบต่อการให้บริการของเครื่องแม่ข่าย จึงมีกระบวนการโจมตีที่ ถูกเรียกว่าการโจมตีแบบแยกส่วนหรือ มีลักษณะแฝงตัวไปยังผู้ใช้บริการรายอื่นและทำการโจมตีเข้าสู่เครื่องแม่ข่ายในช่วงเวลาใกล้เคียงกันและการโจมตีดังกล่าวอาจส่งผลให้เห็นได้ยากในการเชื่อมต่อระหว่างเครือข่ายเพราะมีการป้องกันจากอุปกรณ์จัดเส้นทางและไฟร์วอลล์ แต่หากเกิดขึ้นภายในเครือข่ายภายในอาจส่งผลกระทบที่ร้ายแรงกว่าและป้องกันได้ยาก โดยผู้ดูแลต้องสามารถแยกระดับข้อมูลระหว่างการใช้บริการทั่วไปกับการโจมตี จากประเด็นดังกล่าวกลุ่มข้าพเจ้า นำโปรแกรม Low Orbit Ion Cannon (LOIC) มาใช้ในการตีเป้าหมาย ทำให้เครื่องเป้าหมายทำงานช้าลงจากการใช้โปรแกรม Low Orbit Ion Cannon (LOIC)

3. ประโยชน์ที่จะได้รับจากโครงการ

3.1. ทำให้ผู้ศึกษาเข้าใจระบบการทำงานของ DDoS

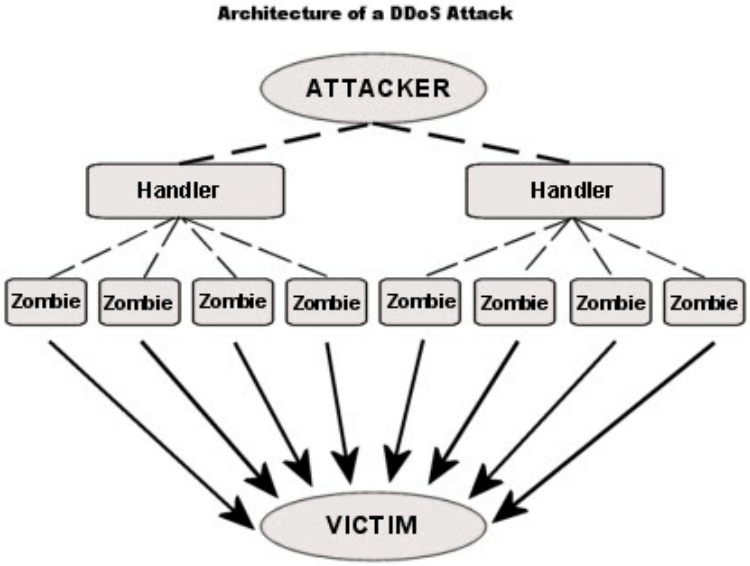
3.2. ให้ผู้ศึกษาเข้าใจการโจมตีของระบบ DDoS

3.3. ให้ผู้ศึกษาเข้าใจการป้องกันของระบบ DDoS

4. ทฤษฎีพื้นฐาน และวรรณกรรมที่เกี่ยวข้อง [1]

การโจมตีแบบ Distributed Denial of Service (DDoS) มีจุดประสงค์เพื่อให้ระบบหยุดการทำงานไม่สามารถใช้เครื่องคอมพิวเตอร์ได้ทั้งระบบหรือเครื่องเดียว ๆ เคยมีเหตุการโจมตีแบบนี้เป็นตัวอย่างจริงมากับประเทศเกาหลีใต้ เมื่อปี 2552 มีแฮกเกอร์ยิง DDoS ถล่มเครือข่ายคอมพิวเตอร์และเว็บไซต์หน่วยงานรัฐบาลเกาหลีใต้ แฮกเกอร์ไม่ทราบสัญชาติได้ส่งข้อมูลเข้าไปทำลายระบบเน็ตเวิร์ก จนเว็บไซต์ใช้งานไม่ได้นานกว่า 4 ชั่วโมง เว็บไซต์เกาหลีใต้ที่ถูกโจมตีไม่ใช่เว็บไซต์ทั่วไป แต่เป็นเว็บไซต์ของกระทรวงกลาโหม เว็บไซต์ทำเนียบประธานาธิบดี ในไทยก็มี ในช่วงที่ปัญหาการเมืองกำลังคุกรุ่นที่ผ่านมาเว็บ ICT ก็เคยถูกโจมตีจนระบบล่ม ไม่สามารถใช้งานได้อยู่หลายชั่วโมง

ผู้ที่โจมตีแบบ DDoS มักจะนำเครื่องมือที่จะใช้ในการโจมตีไปติดตั้งบนคอมพิวเตอร์ที่ถูกเจาะไว้แล้ว คอมพิวเตอร์ที่ได้รับเครื่องมือนี้เข้าไปจะเรียกว่า ซอมบี้ ซึ่งเมื่อมีจำนวนพอสมควรก็จะระดมส่งข้อมูลในรูปแบบที่ควบคุมได้โดยผู้ควบคุมการโจมตีไปยัง เหยื่อหรือเป้าหมายที่ต้องการ ซึ่งการโจมตีรูปแบบนี้มักจะก่อให้เกิดการใช้แบนด์วิดธ์อย่างเต็มที่จนผู้ อื่นไม่สามารถใช้งานได้ตามปกติ หรือทำให้ระบบที่ถูกโจมตีไม่มีทรัพยากรเหลือพอที่จะให้บริการผู้ใช้ธรรมดาได้

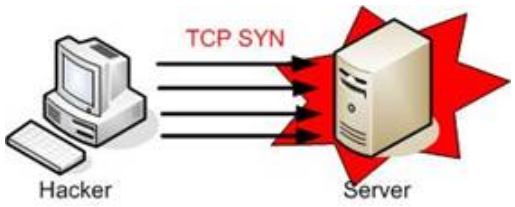


รูปแบบการโจมตี

เครื่องมือที่ใช้โจมตี แบบ DDoS มีใช้กันอย่างแพร่หลายมานานหลายปีแล้วย้อนหลังเป็น 10 ปีมาแล้ว (แต่บรรดาผู้ผลิตอุปกรณ์คอมพิวเตอร์ต่างก็มีวิธีป้องกันการโจมตีเช่นเดียวกัน) รูปแบบการโจมตีที่นิยมใช้กันก็มีอย่างSYN flood, UDP flood, ICMP flood, Smurf, Fraggle เป็นต้น ซึ่งมีรายละเอียดโดยสังเขปดังนี้

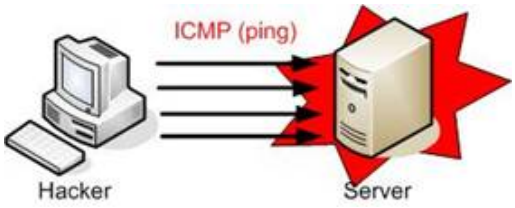
1. การโจมตีแบบ SYN Flood

เป็นการโจมตีโดยการส่ง แพ็คเก็ต TCP ที่ตั้งค่า SYN บิตไว้ไปยังเป้าหมาย เสมือนกับการเริ่มต้นร้องขอการติดต่อแบบ TCP ตามปกติ (ผู้โจมตีสามารถปลอมไอพีของ source address ได้) เครื่องที่เป็นเป้าหมายก็จะตอบสนองโดยการส่ง SYN-ACK กลับมายัง sourceIP address ที่ระบุไว้ ซึ่งผู้โจมตีจะควบคุมเครื่องที่ถูกระบุใน sourceIP address ไม่ให้ส่งข้อมูลตอบกลับ ทำให้เกิดสภาวะ half-open ขึ้นที่เครื่องเป้าหมาย หากมีการส่ง SYN flood จำนวนมาก ก็จะทำให้คิวของการให้บริการของเครื่องเป้าหมายเต็ม ทำให้ไม่สามารถให้บริการตามปกติได้ นอกจากนี้ SYN flood ที่ส่งไปจำนวนมาก ยังอาจจะทำให้เกิดการใช้แบนด์วิดธ์อย่างเต็มที่อีกด้วย



2. การโจมตีแบบ ICMP Flood

เป็นการส่งแพ็คเก็ต ICMP ขนาดใหญ่จำนวนมากไปยังเป้าหมาย ทำให้เกิดการใช้งานแบนด์วิดธ์เต็มที่



3. การโจมตีแบบ UDP Flood

เป็นการส่งแพ็คเก็ต UDP จำนวนมากไปยังเป้าหมาย ซึ่งทำให้เกิดการใช้แบนด์วิดธ์อย่างเต็มที่ และหรือทำให้ทรัพยากรของเป้าหมายถูกใช้ไปจนหมดโดยจะส่ง UDP packet ไปยัง port ที่กำหนดไว้ เช่น 53 (DNS)

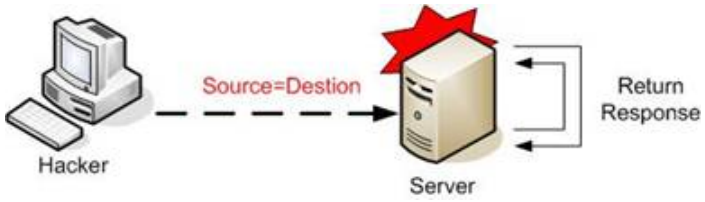
4. การโจมตีแบบ Teardrop

โดยปกติเราเตอร์จะไม่ยอม ให้แพ็กเก็ตขนาดใหญ่ผ่านได้ จะต้องทำ Fragment เสียก่อนจึงจะยอมให้ผ่านได้ และเมื่อผ่านไปแล้วเครื่องของผู้รับปลายทางจะนำแพ็กเก็ตที่ถูกแบ่งออกเป็น ชิ้นส่วนต่าง ๆ ด้วยวิธีการ Fragment มารวมเข้าด้วยกันเป็นแพ็กเก็ตที่สมบูรณ์ การที่สามารถนำมารวมกันได้นี้จะต้องอาศัยค่า Offset ที่ปรากฏอยู่ในแพ็กเก็ตแรกและแพ็กเก็ตต่อ ๆ ไปสำหรับการโจมตีแบบ Teardrop นี้ ผู้โจมตีจะส่งค่า

Offset ในแพ็กเก็ตที่สองและต่อ ๆ ไปที่จะทำให้เครื่องรับปลายทางเกิดความสับสน หากระบบปฏิบัติการไม่สามารถรับมือกับปัญหานี้ก็จะทำให้ระบบหยุดการทำงานในทันที

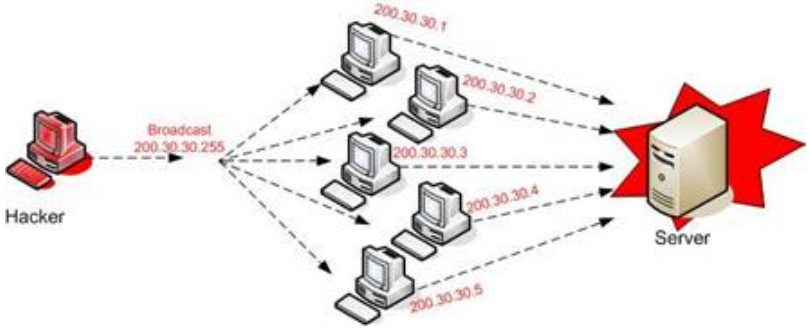
5. การโจมตีแบบ Land Attack

ลักษณะการโจมตีประเภทนี้ เป็นการส่ง SYN ไปที่เครื่องเป้าหมายเพื่อขอการเชื่อมต่อ ซึ่งเครื่องที่เป็นเป้าหมายจะต้องตอบรับคำขอการเชื่อมต่อด้วย SYN ACK ไปที่เครื่องคอมพิวเตอร์ต้นทางเสมอ แต่เนื่องจากว่า IP Address ของเครื่องต้นทางกับเครื่องที่เป็นเป้าหมายนี้มี IP Address เดียวกัน โดยการใช้วิธีการสร้าง IP Address ลวง (โดยข้อเท็จจริงแล้วเครื่องของ Hacker จะมี IP Address ที่ต่างกับเครื่องเป้าหมายอยู่แล้ว แต่จะใช้วิธีการทางซอฟต์แวร์ในการส่งแพ็กเก็ตที่ประกอบด้วยคำขอการเชื่อมต่อ พร้อมด้วย IP Address ปลอม) ซึ่งโปรโตคอลของเครื่องเป้าหมายไม่สามารถแยกแยะได้ว่า IP Address ที่เข้ามาเป็นเครื่องปัจจุบันหรือไม่ ก็จะทำการตอบสนองด้วย SYN ACK ออกไป หากแอดเดรสที่ขอเชื่อมต่อเข้ามาเป็นแอดเดรสเดียวกับเครื่องเป้าหมาย ผลก็คือ SYN ACK นี้จะย้อนเข้าหาตนเอง และเช่นกันที่การปล่อย SYN ACK แต่ละครั้งจะต้องมีการปันส่วนของหน่วยความจำเพื่อการนี้จำนวนหนึ่ง ซึ่งหากผู้โจมตีส่งคำขอเชื่อมต่อออกมาอย่างต่อเนื่องก็จะเกิดปัญหาการจัดสรรหน่วยความจำ



6. Smurf

ผู้โจมตีจะส่ง ICMP Echo Request ไปยัง broadcast address ในเครือข่ายที่เป็นตัวกลาง (ปกติจะเรียกว่า amplifier) โดยปลอม sourceIP address เป็น IP address ของระบบที่ต้องการโจมตี ซึ่งจะทำให้เครือข่ายที่เป็นตัวกลางส่ง ICMP Echo Reply กลับไปยัง IP address ของเป้าหมายทันที ซึ่งทำให้มีการใช้งานแบนด์-วิดธ์อย่างเต็มที่



ความเสียหายที่เกิดโดยการโจมตีในรูปแบบ DoS

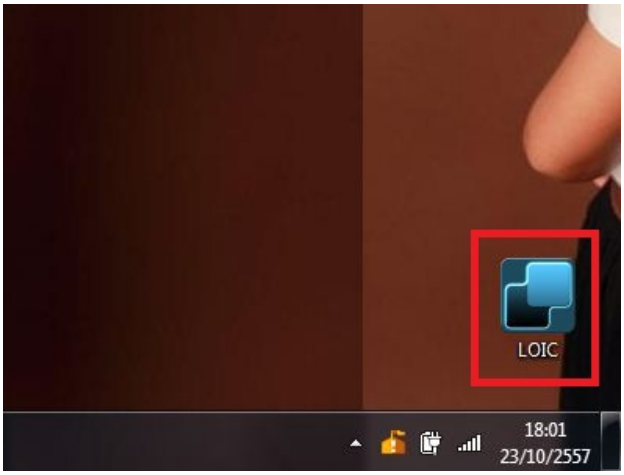
ความเสียหายที่เกิดจาก DoS ส่งผลให้ผู้ใช้งานแต่ละส่วนไม่เหมือนกัน?แล้วแต่ว่าเขาจะอยู่ในส่วนใด เช่น เป็นผู้เข้าไปใช้งาน?เป็นพนักงานในองค์กรที่โดนโจมตีหรือเป็น เจ้าของเครื่องที่ถูกใช้ในการโจมตี

หรือจะมองในแง่ขององค์กรที่โดนโจมตี ทุกๆ ฝ่ายล้วนแล้วแต่เป็นฝ่ายเสียทั้งนั้น?ยกเว้นคนที่ทำให้เหตุการณ์นี้ เกิดขึ้น หรือคนที่เป็นคนบงการอยู่เบื้องหลังเท่านั้นที่ได้ประโยชน์จากการโจมตีนั้น

5. วิธีการดาเนินโครงการ

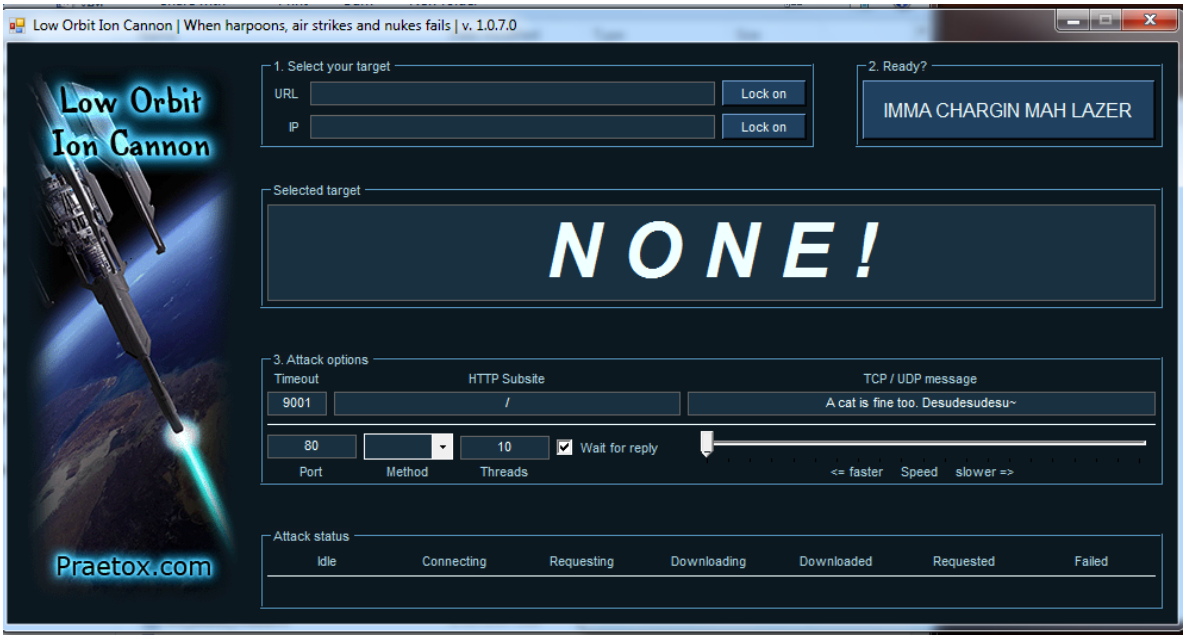
เครื่องมือและอุปกรณ์ที่ใช้ในการทดสอบในโครงการนี้ สามารถแบ่งออกเป็น 2 ส่วน ส่วนแรกคือโปรแกรมที่ ใช้สร้างการโจมตีเครือข่ายทั้งหมด 2 เครื่อง เครื่องที่ 1 และเครื่องที่ 2 ใช้โจมตี และส่วนที่ 2 คือเครื่องที่ 3 คือเครื่องถูกโจมตี เครื่องที่ 4 ใช้ทดสอบเครื่องที่ถูกโจมตี ว่าสามารถใช้งานได้หรือไม่

- ผู้ใช้เปิดโปแกรม Low Orbit Ion Cannon (LOIC)

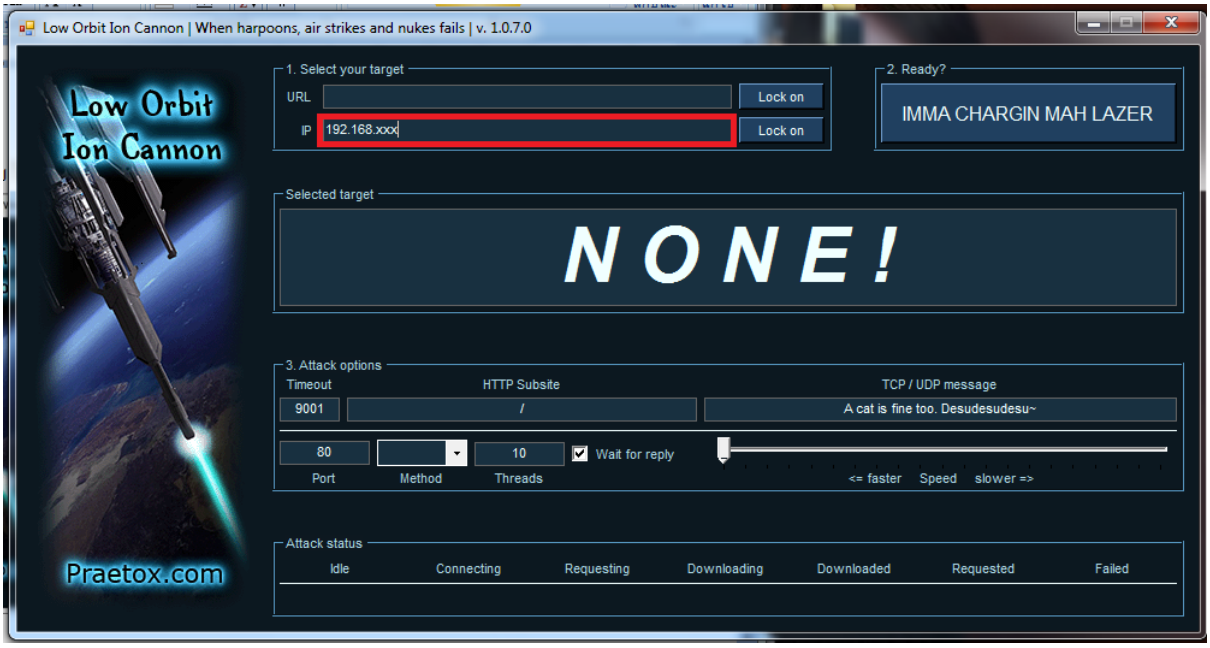


หมายเหตุ : เครื่องที่ 1 เครื่องที่ 2 ใช้งานเหมือนกัน

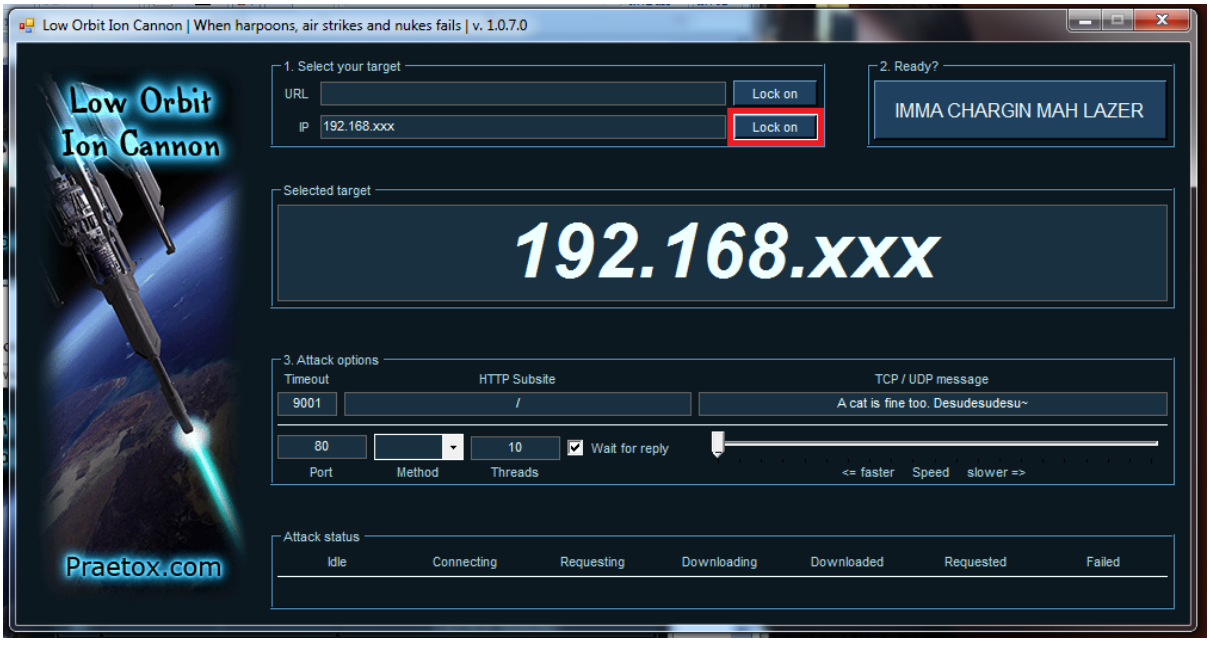
- ผู้ใช้เปิดโปรแกรม Low Orbit Ion Cannon (LOIC) จะมีหน้าจอดังนี้



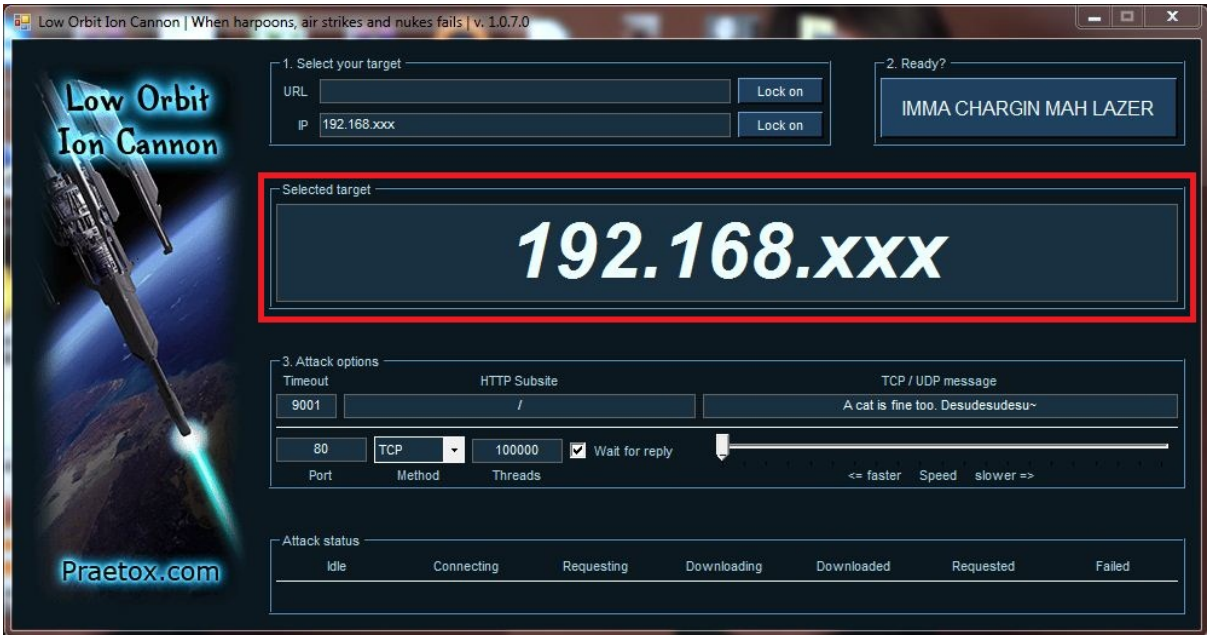
- ผู้ใช้ กรอกเลขไอพี ที่จะทำการโจมตี



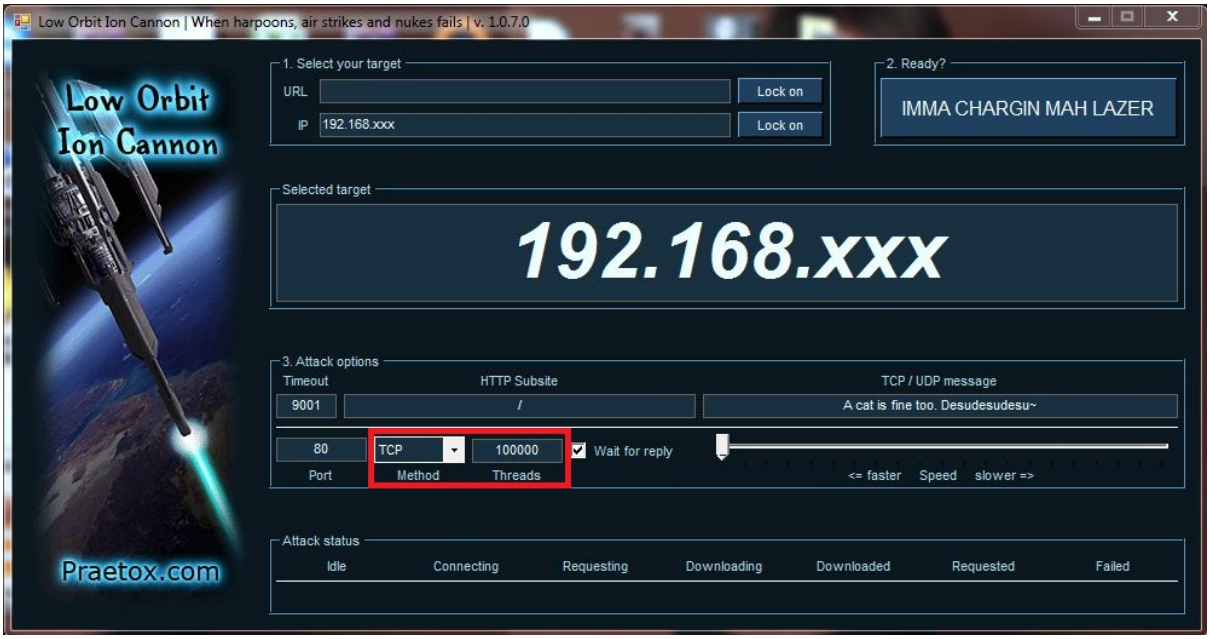
- ผู้ใช้กดที่ปุ่ม Lock on เพื่อยืนยันการโจมตี



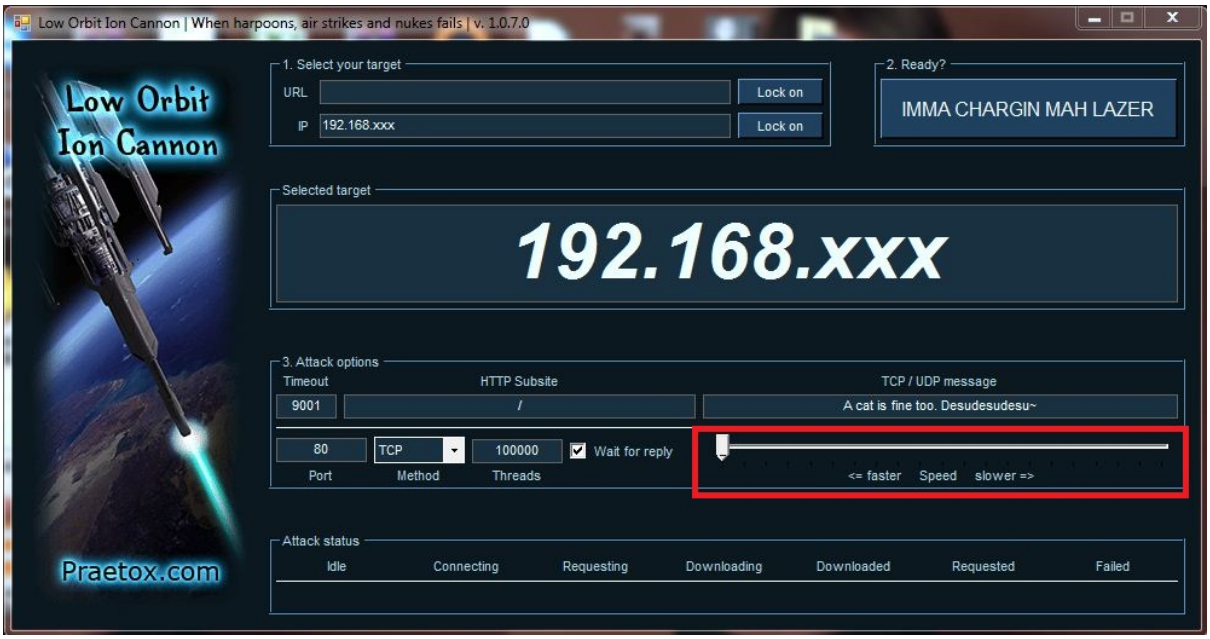
- เมื่อกดยืนยันเสร็จแล้ว โปรแกรมจะแสดงเลขไอพีที่ทำการโจมตี ที่หน้าจอโปรแกรม



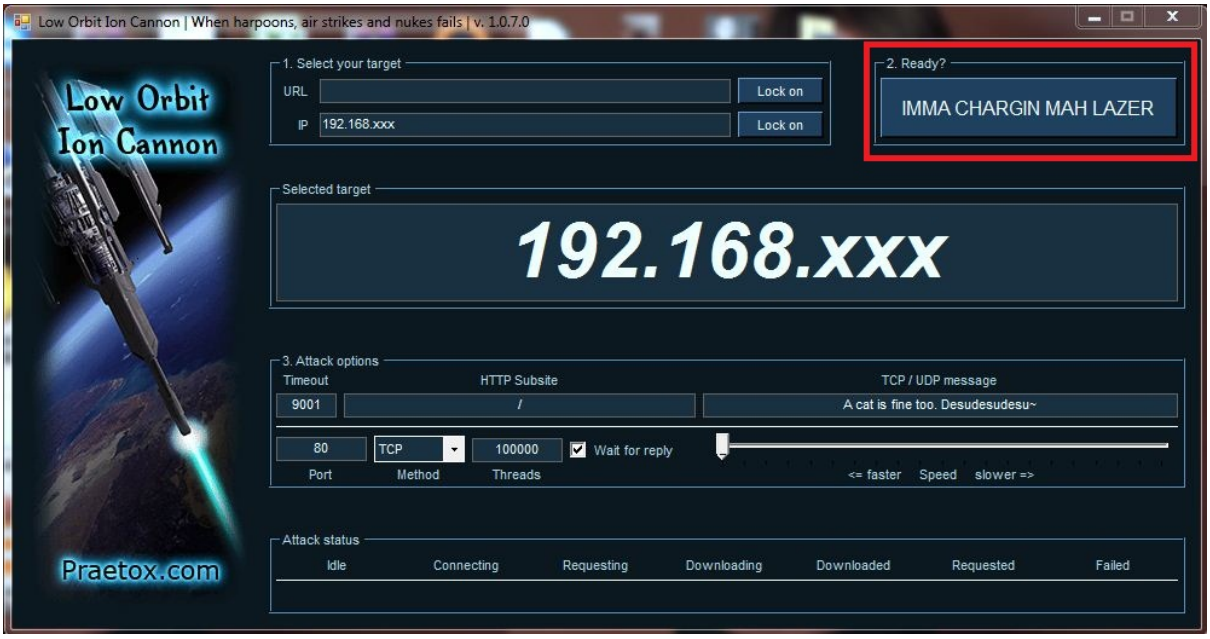
- ตั้งค่า Method เป็น TCP และ Threads เป็น 100000



- ผู้ใช้เลือกความเร็วที่ทำการโจมตี ตั้งค่าเป็น Faster

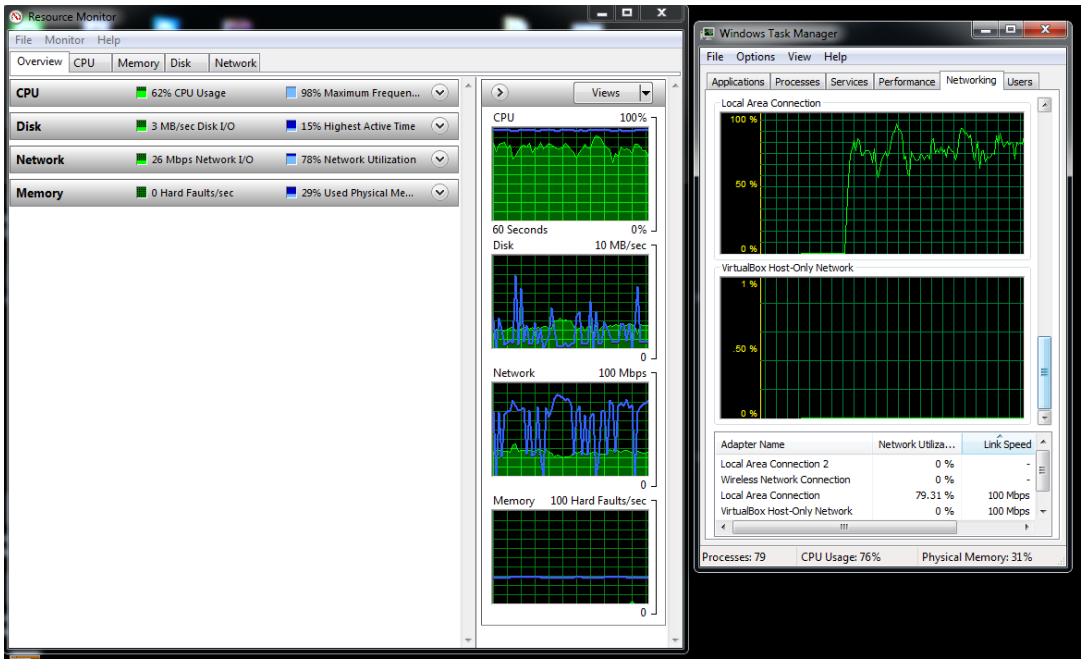


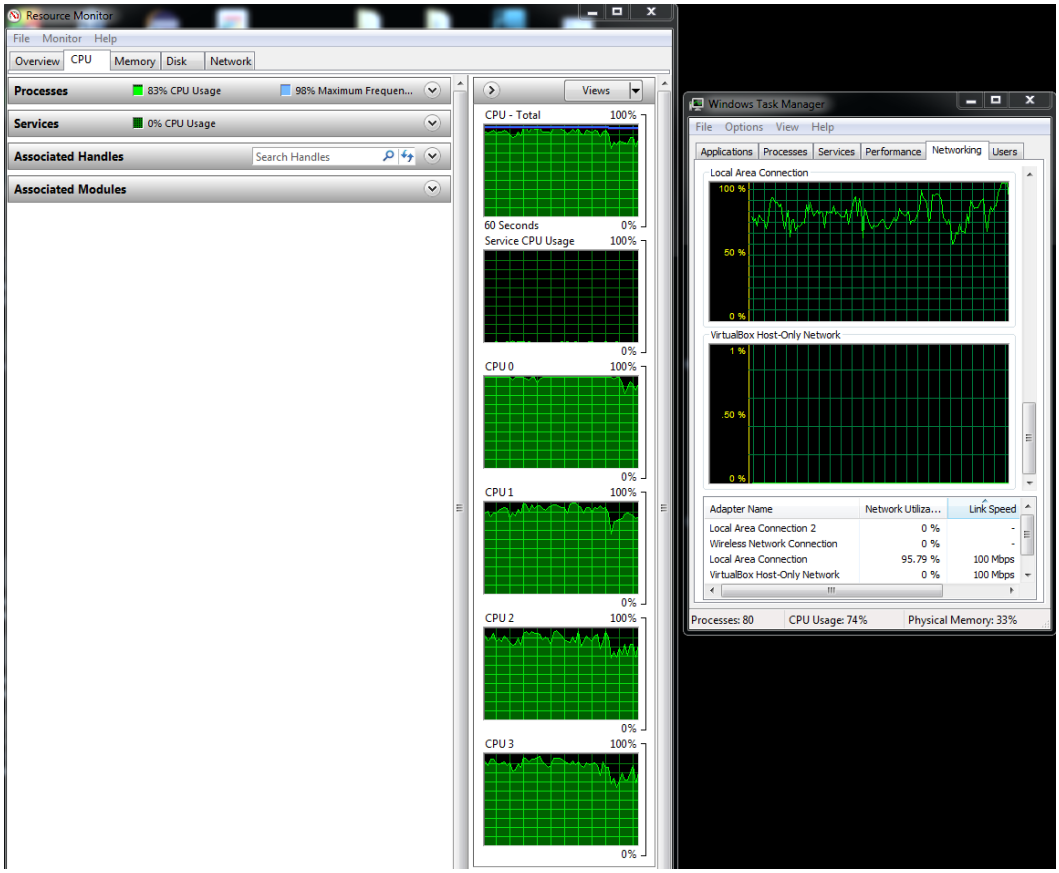
- เมื่อผู้ใช้ตั้งค่าเสร็จสิ้น ผู้ใช้ทำการกดที่ปุ่ม IMMA CHARGIN LAZER เพื่อทำการใช้งานโปรแกรม

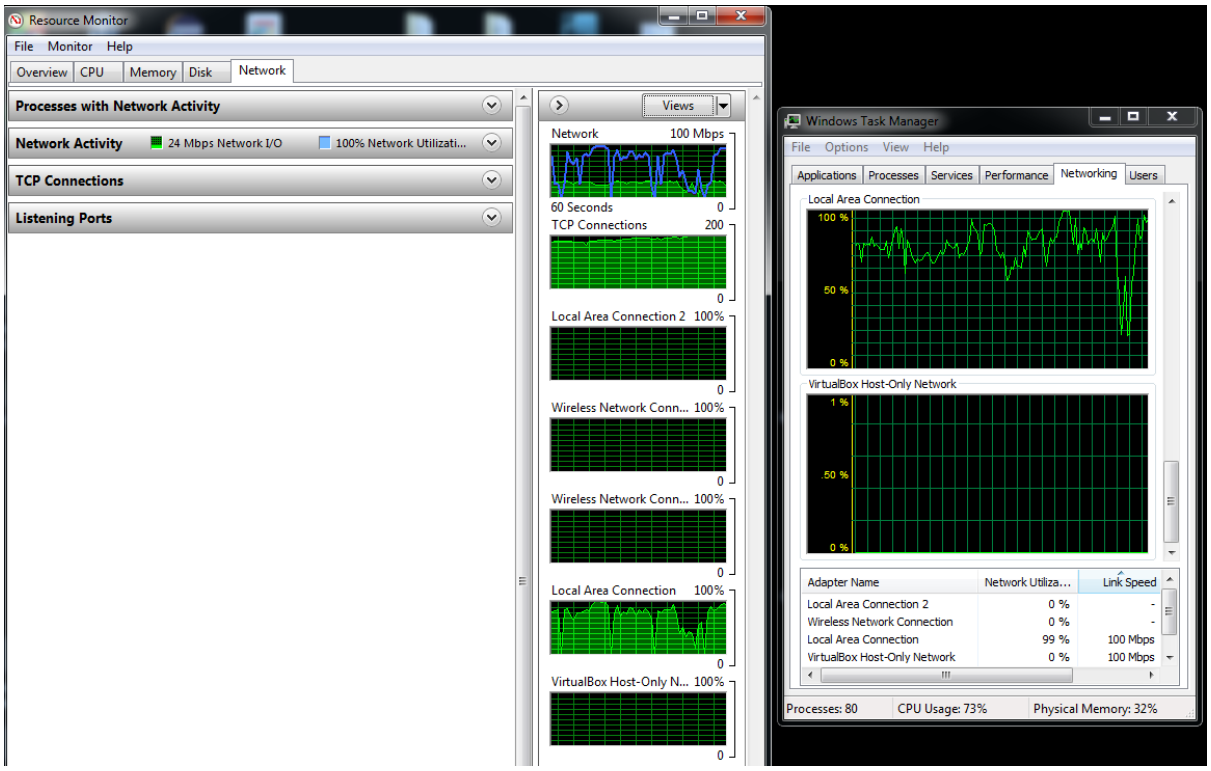


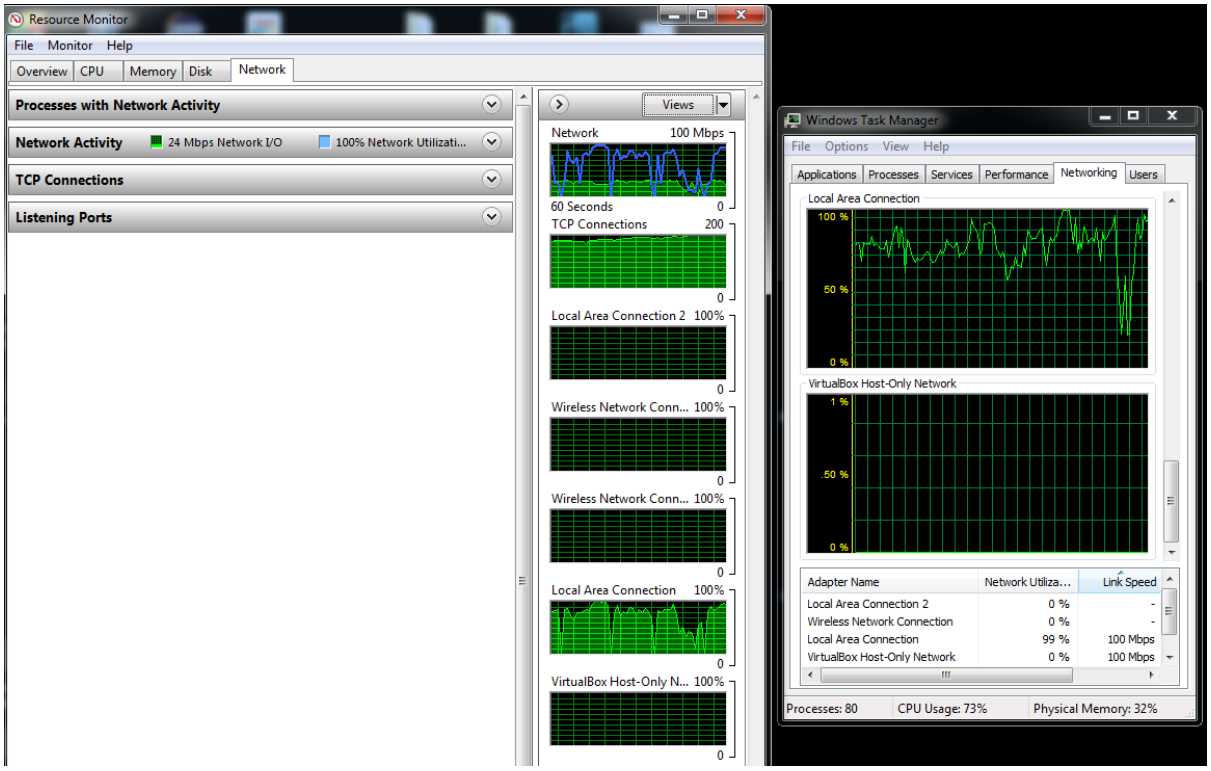
Task Manager Monitor Server

“ หน้าจอ Monitor ของเครื่องที่ถูกโจมตี จะสังเกตว่า มีการทำงานเพิ่มขึ้น “






Resource Monitor
File Monitor Help
Overview CPU Memory Disk Network
Processes with Network Activity
Network Activity 24 Mbps Network I/O 100% Network Utilizati...
TCP Connections
Listening Ports
Views
Network 100 Mbps
60 Seconds 0
TCP Connections 200
Local Area Connection 2 100%
Wireless Network Conn... 100%
Wireless Network Conn... 100%
Local Area Connection 100%
VirtualBox Host-Only N... 100%
Windows Task Manager
File Options View Help
Applications Processes Services Performance Networking Users
Local Area Connection
VirtualBox Host-Only Network
Adapter Name Network Utiliza... Link Speed
Local Area Connection 2 0 % -
Wireless Network Connection 0 % -
Local Area Connection 99 % 100 Mbps
VirtualBox Host-Only Network 0 % 100 Mbps
Processes: 80 CPU Usage: 73% Physical Memory: 32%


Resource Monitor
File Monitor Help
Overview CPU Memory Disk Network
Processes with Network Activity
Network Activity 24 Mbps Network I/O 100% Network Utilizati...
TCP Connections
Listening Ports
Views
Network 100 Mbps
60 Seconds 0
TCP Connections 200
Local Area Connection 2 100%
Wireless Network Conn... 100%
Wireless Network Conn... 100%
Local Area Connection 100%
VirtualBox Host-Only N... 100%
Windows Task Manager
File Options View Help
Applications Processes Services Performance Networking Users
Local Area Connection
VirtualBox Host-Only Network
Adapter Name Network Utiliza... Link Speed
Local Area Connection 2 0 % -
Wireless Network Connection 0 % -
Local Area Connection 99 % 100 Mbps
VirtualBox Host-Only Network 0 % 100 Mbps
Processes: 80 CPU Usage: 73% Physical Memory: 32%

6. สรุปโครงการ

6.1 สามารถทำการโจมตีเครื่องเป้าหมายได้สำเร็จ

6.2 สามารถเข้าใจระบบการทำงานของโปรแกรม Low Orbit Ion Cannon (LOIC) ได้

7. อ้างอิง

[1] Augie. ทำความรู้จักกับ Distributed Denial of Service (DDoS). (2555). ค้นเมื่อ 23 ตุลาคม 2557, จาก http://notebookspec.com/ทำความรู้จักกับ-distributed-denial-of-service-ddos/36287.