ขอบเขตของงาน(Terms of Reference : TOR)
การจัดซื้อระบบตรวจจับและป้องกันการโจมตีเครือข่ายจากภายนอก DDoS
(Distributed Denial of Service)
ของสำนักงาน กสทช. จำนวน ๑ ระบบ

**๑. หลักการและเหตุผล**

ในปัจจุบันแนวโน้มของภัยคุกคามทางไซเบอร์มีความรุนแรง ซับซ้อน และเพิ่มมากขึ้นอย่างรวดเร็ว ประกอบกับการก้าวเข้าสู่สังคมเศรษฐกิจดิจิตอลของหน่วยงานภาครัฐในประเทศไทย ทำให้หน่วยงานมีความจำเป็นต้องเตรียมตัวในหลายด้าน ทั้งด้านโครงสร้างพื้นฐานที่ต้องสามารถรองรับการใช้งานได้เป็นอย่างดี การสนับสนุนให้ประชาชนเข้าถึงข้อมูลและบริการของภาครัฐได้อย่างต่อเนื่อง และการส่งเสริมการสร้างมาตรฐานความปลอดภัยให้สามารถรับมือกับภัยคุกคามที่รุนแรงและซับซ้อนได้

ในช่วงระยะเวลาที่ผ่านมา ผู้โจมตีมักจะมีความมุ่งหวังให้เกิดหยุดชะงักการให้บริการข้อมูลต่างๆ ภายในองค์กร ซึ่งเทคนิคที่ใช้จะเรียกว่า DDoS (Distributed Denial of Service) สำหรับประเทศไทยเคยเกิดเหตุการณ์ประท้วงเรื่องของ Single Gateway ซึ่งมีการใช้เทคนิค DDoS ในการประท้วงเพื่อแสดงออกทางการเมืองในรูปแบบหนึ่ง ซึ่งเป้าประสงค์หลักของการโจมตีเครือข่ายแบบ DDoS คือการทำให้เครื่องแม่ข่ายหรือเครื่องที่ให้บริการ (Server) ไม่สามารถให้บริการได้ตามปกติ วิธีการคือการมุ่งเป้าประสงค์ไปที่เรื่องของการทำให้เส้นทางเชื่อมต่อนั้นเต็ม หรือเกินขีดความสามารถของเครื่องแม่ข่ายที่จะให้บริการตามปกติได้ และก่อให้เกิดความเสียหายต่อหน่วยงานทั้งที่มีผลเป็นตัวเงิน และยังส่งผลกระทบต่อความน่าเชื่อถือของหน่วยงานอีกด้วย สำนักงาน กสทช. จึงได้มีการจัดซื้อระบบตรวจจับและป้องกันการโจมตีเครือข่ายในลักษณะ DDoS ไว้ใช้งานตั้งแต่ปี ๒๕๕๙ จนถึงปัจจุบันซึ่งมีอายุการใช้งานกว่า ๕ ปี และเริ่มล้าสมัย หากใช้งานต่อไปอาจเกิดการทำงานผิดพลาดหรือชำรุดเสียหาย

จากปัญหาดังกล่าว สำนักงาน กสทช. จึงจำเป็นต้องจัดซื้อระบบตรวจจับและป้องกันการโจมตีเครือข่ายจากภายนอก DDoS (Distributed Denial of Service) ของสำนักงาน กสทช. จำนวน ๑ ระบบ ทดแทนที่ใช้งานในปัจจุบัน เพื่อไม่ให้เกิดหยุดชะงักการให้บริการข้อมูลต่างๆ ภายในองค์กร เมื่อถูกโจมตีจาก DDoS โดยจะต้องมีการตรวจสอบและป้องกันการโจมตีที่มาจากภายนอก ก่อนที่ภัยคุกคามดังกล่าวจะทำให้ระบบไม่สามารถให้บริการได้ ซึ่งจะช่วยทำให้องค์กรสามารถลดความเสี่ยงที่จะเกิดขึ้นกับระบบการให้บริการผ่านอินเตอร์เน็ต เช่น ระบบล่มจนไม่สามารถให้บริการได้ ระบบให้บริการได้ช้าและไม่เสถียร เป็นต้น และเพื่อให้การป้องกันการโจมตีมีประสิทธิภาพสูงสุด นอกจากการป้องกันการโจมตีที่มาจากภายนอกแล้ว ยังควรต้องเฝ้าระวังและป้องกันการโจมตีจากภายในองค์กรออกไปภายนอกองค์กรด้วย

**๒. วัตถุประสงค์**

๒.๑. เพื่อจัดซื้อระบบตรวจจับและป้องกันการโจมตีเครือข่ายจากภายนอก DDoS (Distributed Denial of Service) ของสำนักงาน กสทช. จำนวน ๑ ระบบ ทดแทนที่ใช้งานในปัจจุบัน

๒.๒. เพื่อลดความเสี่ยงและป้องกันการถูกโจมตีจากภัยคุกคามที่อุปกรณ์ป้องกันทั่วไปไม่สามารถป้องกันได้ อันจะทำให้หน่วยงานเสียหายหรือเสียความชื่อเสียงจากการหยุดชะงักในการให้บริการ

**๓. คุณสมบัติผู้ยื่นข้อเสนอ**

๓.๑. มีความสามารถตามกฎหมาย

๓.๒. ไม่เป็นบุคคลล้มละลาย

๓.๓. ไม่อยู่ระหว่างเลิกกิจการ

๓.๔. ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

๓.๕. ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

๓.๖. มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

๓.๗. เป็นบุคคลธรรมดาหรือนิติบุคคลผู้มีอาชีพขายพัสดุที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

๓.๘. ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่ สำนักงาน กสทช. ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

๓.๙. ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทยเว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

๓.๑๐. ผู้ยื่นข้อเสนอต้องลงทะเบียนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement : e - GP) ของกรมบัญชีกลาง

๓.๑๑. ผู้ยื่นข้อเสนอต้องได้รับการแต่งตั้งให้เป็นตัวแทนจำหน่ายจากผู้ผลิต สาขาของผู้ผลิต หรือตัวแทนจำหน่ายในประเทศไทย โดยให้ยื่นหนังสือแต่งตั้งพร้อมกับการยื่นข้อเสนอ

**๔. รายละเอียดคุณลักษณะเฉพาะ**

**๔.๑. ข้อกำหนดทั่วไป**

๔.๑.๑. ผู้ขายจะต้องสำรวจ ออกแบบ จัดหา การติดตั้งเชื่อมโยงอุปกรณ์ต่างๆ ทั้ง Hardware, Software และอุปกรณ์อื่น ๆ ที่จำเป็นและจัดทำเป็นแผนการดำเนินงานส่งให้สำนักงาน กสทช. ภายใน ๓๐ วัน นับถัดจากวันลงนามในสัญญา เพื่อให้ความเห็นชอบ ก่อนดำเนินการขั้นต่อไป

๔.๑.๒. ผู้ขายจะต้องดำเนินการ ติดตั้ง เชื่อมโยงและปรับแต่งอุปกรณ์เครือข่ายคอมพิวเตอร์ที่เกี่ยวข้องที่มีใช้งานในปัจจุบันได้ดีให้สามารถทำงานร่วมกับระบบฯ และอุปกรณ์ต่างๆ ที่จัดหาในครั้งนี้ให้สามารถทำงานได้ อย่างถูกต้องและมีประสิทธิภาพ

๔.๑.๓. ผู้ขายจะต้องส่งมอบฮาร์ดแวร์และซอฟท์แวร์ ดำเนินการตั้งค่าการใช้งาน พร้อมส่งเอกสาร ดังนี้

- แผนผังโครงสร้างการเชื่อมต่ออุปกรณ์ต่าง ๆ (Infrastructure diagram) ของระบบทั้งหมดตามที่เสนอในโครงการ
- เอกสารแสดงการกำหนดค่าการติดตั้ง (Configuration) ของระบบทั้งหมด ตามที่เสนอในโครงการ

๔.๑.๔. ผู้ขายจะต้องดำเนินการจัดฝึกอบรมสำหรับผู้ดูแลระบบ จำนวนอย่างน้อย ๒ คน และผู้ใช้งานระบบ จำนวนอย่างน้อย ๑๐ คน ให้เจ้าหน้าที่ สำนักงาน กสทช.

๔.๑.๕. หากต้องมี Hardware หรือ Software อื่นที่จำเป็นเพิ่มเติม เพื่อให้ระบบฯ สามารถใช้งานได้อย่างสมบูรณ์ ผู้ขายต้องจัดหา Hardware หรือ Software ที่เพิ่มเติมนั้นและเป็นผู้รับภาระค่าใช้จ่ายเองทั้งหมด

๔.๑.๖. การดำเนินการใด ๆ ไม่ว่าจะเป็นส่วนของ Hardware และ Software ที่ผู้ขาย เสนอหากมีปัญหาเกี่ยวกับลิขสิทธิ์ ผู้ขายจะต้องดำเนินการขออนุญาตทำการตกลงอย่างอื่นอย่างใดกับบุคคลผู้เป็นเจ้าของลิขสิทธิ์เพื่อให้สามารถใช้ลิขสิทธิ์นั้นๆ ได้อย่างถูกต้องตามกฎหมาย โดยให้ถือเป็นภาระหน้าที่ของผู้ขายเพียงฝ่ายเดียวและเป็นผู้รับภาระค่าใช้จ่ายเองทั้งหมด

**๔.๒. ข้อกำหนดทางด้านเทคนิค**

๔.๒.๑. ฮาร์ดแวร์ของระบบตรวจจับและป้องกันการโจมตีเครือข่ายจากภายนอก DDoS (Distributed Denial of Service) มีคุณสมบัติดังนี้

๔.๒.๑.๑. อุปกรณ์ที่นำเสนอต้องออกแบบสำหรับทำหน้าที่ตรวจจับและหยุดยั้งการโจมตีประเภท Distributed Denial Of Service (DDoS) โดยเฉพาะโดยต้องไม่ใช่อุปกรณ์ IPS หรือ Firewall หรือ ADC ที่สามารถทำหน้าที่นี้ได้

๔.๒.๑.๒. อุปกรณ์ที่นำเสนอจะต้องมี Throughput license ไม่น้อยกว่า ๘ Gbps

๔.๒.๑.๓. สามารถป้องกันการโจมตีสูงสุด (Max Mitigation Throughput) ได้ไม่น้อยกว่า ๒๐ Gbps และ Max DDoS Flood Attack Prevention Rate ได้ไม่น้อยกว่า ๒๕,๐๐๐,๐๐๐ pps

๔.๒.๑.๔. ในกรณีที่มีโจมตีมากกว่า Max Mitigation throughput ของอุปกรณ์ จะต้องสามารถเปลี่ยนเส้นทางของการโจมตี ไปยัง Scrubbing Center ของผลิตภัณฑ์เดียวกันกับอุปกรณ์ที่นำเสนอ ได้โดยอัตโนมัติ และสามารถรองรับ Traffic การโจมตีไม่ต่ำกว่า ๖ Tbps และสามารถเปลี่ยนเส้นทาง clean traffic หลังจากจัดการป้องกัน มาแล้ว ได้ไม่น้อยกว่า ๑๐๐Mbps โดยจะต้องรองรับจำนวนชุด IP ในการป้องกัน ไม่น้อยกว่า ๒๔ network segment (BGP) หรือจำนวนชุด IP ไม่น้อยกว่า ๕ IP addresses (DNS) โดยผู้ยื่นข้อเสนอจะต้องนำเสนอ Ticket ในการ Diversion ไปยัง Cloud Scrubbing Center ไม่น้อยกว่า ๑ ครั้ง

๔.๒.๑.๕. มี Inspection ports ๑๐G SFP+ จำนวนไม่น้อยกว่า ๘ พอร์ต มาพร้อมกับ transceiver แบบ ๑๐G based-SR จำนวนไม่น้อยกว่า ๔ ชุด และสามารถ Bypass การทำงานในกรณีที่อุปกรณ์มีปัญหาไม่น้อยกว่า ๒ Segment หรือเสนออุปกรณ์ External bypass เพิ่มเติม

๔.๒.๑.๖. มีพอร์ตแบบ ๑๐/๑๐๐/๑๐๐๐ Copper Ethernet ใช้ในการบริหารจัดการ (Management) อย่างน้อย ๑ พอร์ต

๔.๒.๑.๗. สามารถทำงานได้ทั้งในแบบ In-line Mode และ Copy port Monitoring หรือ Span port monitoring ได้

๔.๒.๑.๘. สามารถป้องกันการโจมตีประเภท DoS/DDoS Attack โดยใช้ Behavioural based และ Signature based หรือ Host behavioral protection ได้เป็นอย่างน้อย

๔.๒.๑.๙. สามารถป้องกันการโจมตีประเภท Application DoS เช่น HTTP Flood Attacks , DNS Flood Attacks และ SYN Flood Attacks ได้

๔.๒.๑.๑๐. สามารถป้องกันการโจมตี หรือ Block เป็นแบบ IP หรือแบบประเทศ Location-Based Mitigation

๔.๒.๑.๑๑. สามารถพิสูจน์ความถูกต้องของการจราจร (Traffic Authentication) ด้วยวิธีการ Challenge/Response ผ่าน Protocol HTTP, และ HTTPS ได้

๔.๒.๑.๑๒. สามารถป้องกันการโจมตีแบบ TLS หรือ SSL ได้ เช่น HTTPS Flood, SSL vulnerabilities โดยใช้การ inspect encrypt traffic เพื่อตรวจสอบการโจมตีและป้องกันด้วยการทำ Challenge-response mechanism โดยรองรับTLS/SSL(HTTPS) ไม่น้อยกว่า ๔๕,๐๐๐ CPS

๔.๒.๑.๑๓. อุปกรณ์ที่นำเสนอจะต้องมี Dual hot-swap power supply หรือคุณสมบัติอื่นที่เทียบเคียง

๔.๒.๑.๑๔. อุปกรณ์ที่นำเสนอต้องได้รับการรับรอง IEC ๖๐๙๕๐-๑, RoHS , FCC Part๑๕ (Class A)

๔.๒.๒. ซอฟท์แวร์บริหารจัดการระบบตรวจจับและป้องกันการโจมตีเครือข่ายจากภายนอก DDoS (Distributed Denial of Service) แบบ Virtual Appliance มีคุณสมบัติดังนี้

๔.๒.๒.๑. เป็นระบบบริหารจัดการแยกออกมาจากตัวอุปกรณ์ DDoS Protection เพื่อใช้ในการกำหนด Security Policy หรือ “Configuration or View”

๔.๒.๒.๒. สามารถแสดงผลอย่างน้อยดังนี้

๑. Real-time Monitoring,

๒. Security Analytics Dashboard หรือ System and Security alerts

๓. Customized Reporting,

๔. Advanced Forensics

๔.๒.๒.๓. ต้องมีลิขสิทธ์การใช้งานอย่าถูกต้องตามกฎหมาย

**๕. ระยะเวลาดำเนินการ**

ภายใน ๑๘๐ วัน นับถัดจากวันลงนามในสัญญา

**๖. ระยะเวลาส่งมอบงาน**

ผู้ขายจะต้องส่งมอบระบบและเอกสารทั้งหมด ตามรายละเอียดที่กำหนดในคุณลักษณะเฉพาะข้อ ๔ ให้กับคณะกรรมการตรวจรับพัสดุของสำนักงาน กสทช. ภายใน ๑๘๐ วัน นับถัดจากวันลงนามในสัญญา

**๗. วงเงินที่ใช้ในการจัดหา**

วงเงินรวมทั้งสิ้น ๙,๙๕๑,๐๐๐.- บาท (เก้าล้านเก้าแสนห้าหมื่นหนึ่งพันบาทถ้วน) ซึ่งรวมภาษีมูลค่าเพิ่มและค่าใช้จ่ายทั้งปวงแล้ว โดยเบิกจ่ายจากงบประมาณรายจ่ายประจำปี ๒๕๖๕ รายจ่ายเกี่ยวกับครุภัณฑ์ ที่ดินและสิ่งก่อสร้าง รายการครุภัณฑ์คอมพิวเตอร์ สำนักเทคโนโลยีสารสนเทศ ทั้งนี้ จะลงนามผูกพันในสัญญาได้ก็ต่อเมื่อ งบประมาณรายจ่ายประจำปี ๒๕๖๕ ได้รับการพิจารณาอนุมัติจาก กสทช. และมีผลบังคับใช้แล้วเท่านั้น

**๘. การยื่นข้อเสนอ**

ผู้ยื่นข้อเสนอต้องยื่นข้อเสนอและเสนอราคาทางระบบการจัดซื้อจัดจ้างภาครัฐ (Electronic Government Procurement : e-GP) ตามที่กำหนดไว้ในเอกสารประกวดราคาอิเล็กทรอนิกส์ โดยไม่มีเงื่อนไขใด ๆ ทั้งสิ้น และจะต้องกรอกข้อความให้ถูกต้องครบถ้วน ลงลายมือชื่ออิเล็กทรอนิกส์หรือหลักฐานแสดงตัวตนของผู้ยื่นข้อเสนอในรูปแบบ PDF File (Portable Document Format) โดยจำแนกเอกสารที่ยื่นข้อเสนอ ดังนี้

๘.๑ เอกสารแสดงคุณสมบัติทั่วไปของผู้ยื่นข้อเสนอ ตามคุณสมบัติของผู้ยื่นข้อเสนอ ข้อ ๓.

๘.๒ เอกสารข้อเสนอด้านคุณสมบัติและคุณภาพของพัสดุที่เสนอตามข้อ ๔ ประกอบด้วย

๘.๒.๑ บัญชีรายละเอียดแค็ตตาล็อก แบบรูปรายละเอียด เอกสารประกอบที่เกี่ยวข้อง (Data sheet) จำแนกตามรายการ ชนิด ประเภท ฯลฯ โดยรายการ Hardware, Software และอื่นๆ ที่ระบุในบัญชีรายละเอียด จะต้องสอดคล้องตรงกันกับการแจกแจงรายการพัสดุและราคาต่อหน่วยในเอกสารข้อเสนอด้านราคา และสามารถเปรียบเทียบความถูกต้องตรงกัน

๘.๒.๒ เอกสารการยอมรับข้อกำหนด (Statement of Compliance) มีรายละเอียด

(๑) แสดงรายละเอียดของอุปกรณ์และ หรืองานทั้งหมดที่นำเสนอ/เปรียบเทียบกับข้อกำหนดเป็นรายข้อทุกข้อรวมทั้งข้อย่อย รายละเอียดทั้งหมดที่ปรากฏอยู่ในการยอมรับข้อกำหนดที่ผู้ยื่นข้อเสนอระบุว่า ตรงตามข้อกำหนดหรือดีกว่าข้อกำหนด หรือสามารถทำได้ตามข้อกำหนด หรือ ยินดีดำเนินงานตามข้อกำหนด แล้วแต่กรณีแต่ละหัวข้อ

(๒) การยอมรับข้อกำหนดจะต้องมีความสอดคล้องกับรายละเอียดของเอกสารแค็ตตาล็อก แบบรูปรายละเอียด ฯลฯ และผู้ยื่นข้อเสนอจะต้องระบุให้ชัดเจนว่ารายละเอียดที่อธิบายเกี่ยวกับการยอมรับข้อกำหนดอยู่ ณ ตำแหน่งใดในเอกสารข้อเสนอดังกล่าว โดยแสดงเลขอ้างอิงระบุเลขหัวข้อของข้อกำหนดไว้ในเอกสารข้อเสนอ ณ ตำแหน่งที่มีรายละเอียดอธิบายเกี่ยวกับการยอมรับข้อกำหนดนั้น

ทั้งนี้ หากเอกสารข้อเสนอทางด้านคุณภาพไม่มีรายละเอียดที่อธิบายเกี่ยวกับการยอมรับว่าสามารถทำได้ตามข้อกำหนด หรือคำอธิบายที่ไม่ละเอียดเพียงพอหรือขัดแย้งข้อกำหนด หรือไม่แสดงหนังสือรับรองให้ครบถ้วน สำหนังาน กสทช. สงวนสิทธิ์จะพิจารณาว่า ผู้ยื่นข้อเสนอไม่สามารถทำได้ตามข้อกำหนด (Non-Compliance)

๘.๓ ผู้ยื่นข้อเสนอจะต้องเสนอราคาตามแบบที่กำหนดในเอกสารประกวดราคา พร้อมทั้งจัดทำข้อมูลรายละเอียดอัตราค่าจ้างต่อหน่วยของงานแต่ละรายการหรือแต่ละขั้นงานให้ครบถ้วนชัดเจน โดยราคาที่เสนอเป็นราคารวมค่าภาษีมูลค่าเพิ่มและค่าใช้จ่ายทั้งปวงด้วยแล้ว

๘.๔ การยื่นข้อเสนอดังกล่าว ผู้ยื่นข้อเสนอจะต้องปฏิบัติตามหลักเกณฑ์ เงื่อนไขและวิธีการที่กำหนดในเอกสารการประกวดราคาจัดซื้อจัดจ้างและตามที่กำหนดในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement : e-GP) โดยถูกต้องครบถ้วน

๘.๕ หลังจากยื่นข้อเสนอดังกล่าวแล้ว ผู้ยื่นข้อเสนอจะต้องส่งตัวอย่างพัสดุที่เสนอและทดสอบการทำงาน พร้อมอุปกรณ์และอื่น ๆ ตามที่กำหนดในเอกสารแนบท้ายขอบเขตของงาน ภายในไม่เกิน ๓ วันทำการนับถัดจากวันที่คณะกรรมการประกาศให้เข้าทดสอบ

**๙. เกณฑ์การพิจารณาคัดเลือกข้อเสนอ**

เมื่อสิ้นสุดระยะเวลาการเสนอราคาในระบบอิเล็กทรอนิกส์แล้ว คณะกรรมการประกวดราคาอิเล็กทรอนิกส์จะดำเนินการตามลำดับ ดังนี้

๙.๑ จัดพิมพ์เอกสารข้อเสนอทั้งหมดของผู้ยื่นข้อเสนอทุกรายจากระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement : e- GP) (ยกเว้นเอกสารข้อเสนอด้านราคา) ชุด และลงลายมือชื่อกำกับไว้ทุกแผ่น จำนวน ๑

๙.๒ ตรวจสอบการมีผลประโยชน์ร่วมกัน และความครบถ้วนถูกต้องของเอกสารหลักฐานต่าง ๆ แล้วพิจารณาคัดเลือกรายที่ไม่มีผลประโยชน์ร่วมกัน มีคุณสมบัติและเอกสารหลักฐานต่าง ๆ ครบถ้วนถูกต้องและพิจารณาข้อเสนอด้านเทคนิคต่อไป สำหรับรายที่มีผลประโยชน์ร่วมกัน หรือมีคุณสมบัติ หรือยื่นเอกสารหลักฐานต่าง ๆ ไม่ครบถ้วนถูกต้อง คณะกรรมการฯ จะไม่ทำการประเมินค่าประสิทธิภาพต่อราคาตาม

หลักเกณฑ์ที่กำหนด เว้นแต่เป็นข้อผิดพลาด หรือผิดหลงเพียงเล็กน้อยหรือผิดแผกไปจากเงื่อนไขของเอกสารประกวดราคาอิเล็กทรอนิกส์ในส่วนที่มิใช้สาระสำคัญเฉพาะในกรณีที่พิจารณาเห็นว่าจะเป็นประโยชน์ต่อสำนักงาน กสทช. เท่านั้น

๙.๓ พิจารณาเอกสารข้อเสนอด้านเทคนิคของผู้ยื่นข้อเสนอทุกราย หากผู้ยื่นข้อเสนอรายใดมีคุณสมบัติไม่ถูกต้อง หรือยื่นหลักฐานการยื่นข้อเสนอไม่ถูกต้อง หรือไม่ครบถ้วน หรือยื่นข้อเสนอไม่ถูกต้อง หรือไม่ผ่านการจำลองการทำงานของระบบตามที่กำหนดไว้ทุกหัวข้อ คณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์ จะไม่รับพิจารณาราคาของผู้ยื่นข้อเสนอราคารายนั้น เว้นแต่เป็นข้อผิดพลาด หรือผิดเพียงเล็กน้อย หรือผิดแผกไปจากเงื่อนไขของเอกสารประกวดราคาอิเล็กทรอนิกส์ในส่วนที่มิใช้สาระสำคัญ เฉพาะในกรณีที่พิจารณาเห็นว่าจะเป็นประโยชน์ต่อสำนักงาน กสทช. เท่านั้น

๙.๔ คณะกรรมการฯ จะเชิญให้ผู้ยื่นข้อเสนอทุกรายที่มีคุณสมบัติและยื่นเอกสารครบถ้วนถูกต้องตามข้อ ๙.๒ ข้อเสนอด้านเทคนิค ตามคุณลักษณะเฉพาะ ข้อ ๔ .เข้ามาจำลองการทำงานของระบบฯ โดยจะพิจารณาประเมินค่าประสิทธิภาพจากหัวข้อต่าง ๆ รายละเอียดของวิธีการตามเอกสารแนบท้าย โดยการทดสอบการจำลองการทำงานของระบบฯ ทุกหัวข้อ หากไม่ผ่านข้อหนึ่งข้อใด จะถือว่าข้อเสนอของผู้ยื่นข้อเสนอรายนั้นไม่ผ่านการทดลองการทำงานของระบบ

๙.๕ การส่งตัวอย่างและการทดสอบจำลองการทำงานของระบบตามรายละเอียดแนบท้ายขอบเขตของงานนี้ ทั้งนี้ให้ผู้ยื่นข้อเสนอจัดเตรียมอุปกรณ์และระบบต่างๆ เพื่อจำลองการทำงานของระบบภายใน ๓ วันทำการนับถัดจากวันที่ยื่นข้อเสนอผ่านระบบ e-GP และดำเนินการจำลองการทำงานดังกล่าวให้แล้วเสร็จภายใน ๑ วัน หลังจากการเตรียมอุปกรณ์และระบบต่างๆ

๙.๖ ข้อเสนอที่ผ่านเกณฑ์การพิจารณาตามข้อ ๙.๔ จะได้รับการพิจารณาคัดเลือก และเสนอราคาต่ำสุดจะได้รับการคัดเลือกให้เป็นผู้ชนะการประกวดราคาอิเล็กทรอนิกส์ และคณะกรรมการฯ จะพิจารณาเจรจาต่อรองราคาตามที่เห็นสมควรเพื่อประโยชน์ของสำนักงาน กสทช. ต่อไป

๙.๗ กรณีผู้ได้รับการคัดเลือกไม่ไปทำสัญญาภายในวันเวลาที่กำหนดสำนักงาน กสทช. จะพิจารณาเรียกรายลำดับถัดไปเพื่อเจรจาต่อรองและ/หรือทำสัญญาต่อไป หรืออาจพิจารณายกเลิก การประกาศเชิญชวนเพื่อดำเนินการใหม่ตามวิธีหรือขั้นตอนตามระเบียบที่เกี่ยวข้องต่อไป

**๑๐.เงื่อนไขการชำระเงิน**

สำนักงาน กสทช. จะชำระเงินเมื่อผู้ขายได้ส่งมอบระบบฯและเอกสารทั้งหมดครบถ้วน ตามรายละเอียดขอบเขตงานข้อ ๔. ภายในกรอบระยะเวลาตามรายละเอียดข้อ ๖. และผ่านการตรวจรับจากคณะกรรมการตรวจรับพัสดุของสำนักงาน กสทช. เป็นที่เรียบร้อยแล้ว

**๑๑.เงื่อนไขอื่น ๆ**

๑๑.๑. การบริการ

ผู้ขายต้องจัดให้มีบริการ Help Desk เพื่อรับแก้ไขปัญหาในวันเวลาทำงานของสำนักงาน กสทช. ตั้งแต่ ๐๘.๓๐ – ๑๖.๓๐ น.

๑๑.๒. การรับประกัน

ผู้ขายต้องรับประกัน Hardware และ Software ต่าง ๆ ทั้งหมดที่ส่งมอบเป็นระยะเวลาไม่น้อยกว่า ๑ ปี นับถัดจากวันที่คณะกรรมการตรวจรับพัสดุได้ตรวจรับเป็นที่เรียบร้อยแล้ว ภายในกำหนดเวลารับประกัน จะต้องบำรุงรักษาอุปกรณ์ทั้งโครงการโดยไม่คิดค่าใช้จ่ายใด ๆ ทั้งสิ้น

๑๑.๓. ค่าปรับ

ผู้ขายจะต้องติดตั้งและส่งมอบงานแล้วเสร็จตามสัญญา มิฉะนั้นต้องชำระค่าปรับให้สำนักงาน กสทช. เป็นรายวันในอัตราร้อยละ ๐.๒๐ ของค่าพัสดุที่ยังไม่ได้รับมอบ จนถึงวันที่ผู้ขายได้ส่งมอบงานให้สำนักงาน กสทช. เป็นที่เรียบร้อยแล้ว ในระหว่างที่สำนักงาน กสทช. ยังไม่ได้ใช้สิทธิ์บอกเลิกสัญญานั้น หากสำนักงาน กสทช. เห็นว่าผู้ขายไม่อาจปฏิบัติตามสัญญาต่อไปได้ สำนักงาน กสทช. จะใช้สิทธิ์บอกเลิกสัญญากับเรียกร้องให้ชดใช้ราคาที่เพิ่มขึ้นจากราคาที่กำหนดไว้ในสัญญา ถ้าสำนักงาน กสทช. ดำเนินการโดยการจัดซื้อจากบุคคลอื่นเต็มจำนวน หรือเฉพาะจำนวนที่ขาดส่ง และถ้าสำนักงาน กสทช. ได้แจ้งข้อเรียกร้องให้ชำระค่าปรับไปยังผู้ขายเมื่อครบกำหนดส่งมอบแล้ว สำนักงาน กสทช. มีสิทธิ์ที่จะปรับผู้ขายจนถึงวันบอกเลิกสัญญาได้อีกด้วย

๑๑.๔. การทำสัญญากับผู้ชนะการประกวดราคาอิเล็กทรอนิกส์ สำนักงาน กสทช. จะใช้แบบสัญญาซื้อขายคอมพิวเตอร์ตามแบบที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดตามแบบสัญญาแนบท้ายขอบเขตของงานนี้

เอกสารแนบ

**ความต้องการของการจำลองการทำงานของระบบ**

---

**๑. ขอบเขตความรับผิดชอบการจัดเตรียมการจำลองการทำงานของระบบ**

๑.๑. สถานที่ ณ สำนักงาน กสทช. อาคารจอดรถชั้น ๑ สำนักเทคโนโลยีสารสนเทศ

๑.๒. ผู้ยื่นข้อเสนอจัดเตรียมการจำลองการโจมตีและการทำงาน และเตรียมส่วนประกอบต่างๆ ดังนี้

- อุปกรณ์ป้องกันการโจมตีประเภท Distributed Denial Of Service (DDoS) รุ่นเดียวกับที่นำเสนอในโครงการ
- เครื่องคอมพิวเตอร์แม่ข่ายพร้อมติดตั้ง ซอฟต์แวร์บริหารจัดการ ที่ทำงานร่วมกับอุปกรณ์ DDoS Mitigator
- เครื่องคอมพิวเตอร์ลูกข่าย พร้อมติดตั้งซอฟต์แวร์สำหรับการทดสอบการโจมตี
- อุปกรณ์สำหรับเชื่อมต่อ เช่น Network switch, สาย LAN

๑.๓. ผู้ยื่นข้อเสนอต้องเตรียมความพร้อมสำหรับการจำลองการทำงานของระบบ ดังนี้

๑.๓.๑ ทำการติดตั้งระบบตามข้อ ๑.๒ ให้สามารถทำงานร่วมกันได้อย่างมีประสิทธิภาพ มาให้พร้อม ณ วันที่ทำการทดสอบการจำลองระบบ

๑.๓.๒ จำลองการโจมตีและการทำงานป้องกันของระบบ ตามข้อที่ ๒

๑.๔. ผู้ยื่นข้อเสนอสามารถทดสอบในแต่ละหัวข้อได้ ๒ ครั้ง แต่ละครั้งห่างกันไม่เกิน ๑๕ นาที หากไม่ผ่านครั้งที่ ๑ สำนักงานจะให้ผู้ยื่นข้อเสนอปรับแต่งระบบใหม่ ณ วันที่นำเสนอการจำลองการทำงานของระบบ หากปรับแต่งแล้วไม่สามารถใช้งานได้จะถือว่าไม่ผ่านในข้อนั้น

๒. จำลองการทำงานของระบบ

| 1. การทดสอบการป้องกัน Volumetric Attack | | | |
|---|---|---|---|
| **รูปแบบการโจมตี** | **วัตถุประสงค์** | **รายละเอียดวิธีการ** | **ผลที่ต้องการ** |
| 1.1 UDP Flood - Random Source IP | เพื่อจำลองและทดสอบการป้องกันการโจมตีผ่านโปรโตคอล UDP (NTP) แบบสุ่ม IP ต้นทางในการโจมตี โดยหวังผลให้เครื่องเป้าหมายไม่สามารถใช้งานได้ | พารามิเตอร์ที่ใช้ทดสอบ<br>Network Layer-> SRC IP: random, DST IP: Target<br>Transport Layer-> UDP<br>Session Layer-> DST Port: 123 (NTP), SRC Port: random<br>Application Layer-> None<br>Other Characteristics-> Attack rate: Flood Packet body size: fixed = 100B | ☐ สามารถตรวจจับอัตราการโจมตีได้ |

| 1. การทดสอบการป้องกัน Volumetric Attack | | | |
|---|---|---|---|
| **รูปแบบการโจมตี** | **วัตถุประสงค์** | **รายละเอียดวิธีการ** | **ผลที่ต้องการ** |
| 1.2 UDP Flood - Random Source IP, Random Packet Size | เพื่อจำลองและทดสอบการป้องกันการโจมตีผ่านโปรโตคอล UDP (NTP) พร้อมทั้งสุ่ม IP และขนาดของแพ็ตเกต ต้นทางในการโจมตี โดยหวังผลให้เครื่องเป้าหมายไม่สามารถใช้งานได้ | พารามิเตอร์ที่ใช้ทดสอบ<br>Network Layer-> SRC IP: random, DST IP: Target<br>Transport Layer-> UDP<br>Session Layer-> DST Port: 123 (NTP), SRC Port: 21212<br>Application Layer-> None<br>Other Characteristics-> Attack rate: Flood,<br>Packet body size: random <1000B | ☐ สามารถตรวจจับอัตราการโจมตีได้ |
| 1.3 UDP Flood - Random Layer 4 | เพื่อจำลองและทดสอบการป้องกันการโจมตีผ่านโปรโตคอล UDP แบบสุ่ม IP ต้นทาง-ปลายทาง สุ่ม Port การเชื่อมต่อทั้งปลายทางและต้นทาง สุ่มขนาดของแพ็ตเกตและค่า ttl ในการโจมตี | พารามิเตอร์ที่ใช้ทดสอบ<br>Network Layer-> SRC IP: random, DST IP: 2.2.2.1-10<br>Transport Layer-> UDP<br>Session Layer-> DST Port: random, SRC Port: random<br>Application Layer-> None<br>Other Characteristics-> Attack rate: Flood, Packet body size: random | ☐ สามารถตรวจจับอัตราการโจมตีได้ |

| 1. การทดสอบการป้องกัน Volumetric Attack | | | |
|---|---|---|---|
| **รูปแบบการโจมตี** | **วัตถุประสงค์** | **รายละเอียดวิธีการ** | **ผลที่ต้องการ** |
| 1.4 UDP Fragmented Flood - Random Packet Size | เพื่อจำลองและทดสอบการป้องกันการโจมตีผ่านโปรโตคอล UDP (NTP) แบบการกระจาย โดยมีการสุ่มการส่งแพ็คเกตออกไปเครื่องเป้าหมาย โดยที่ให้มีค่ามากกว่า 1500 ไบต์ โดยหวังผลคือเครื่องเป้าหมายมีการใช้ทรัพยากรอย่างรวดเร็วและไม่สามารถเข้าถึงเครื่องเป้าหมายได้ | พารามิเตอร์ที่ใช้ทดสอบNetwork Layer-> SRC IP: random, DST IP: TargetTransport Layer-> UDP Session Layer-> DST Port: 123 (NTP), SRC Port: 21212 Application Layer-> None Other Characteristics-> Attack rate: Flood, Packet body size: random > 1500B | ☐ สามารถตรวจจับอัตราการโจมตีได้ |
| 1.5 UDP Flood – Carpet Bombing | เพื่อจำลองและทดสอบการป้องกันการโจมตีผ่านโปรโตคอล UDP (IKE/IPSEC) แบบส่งไปยังปลายทางหลายที่ ซึ่งส่วนใหญ่ถูกกำหนด IP เป็นภายในวง subnet เดียวกัน | พารามิเตอร์ที่ใช้ทดสอบ<br>Network Layer-> SRC IP: random, DST IP: 2.2.2.0/24<br>Transport Layer-> UDP<br>Session Layer->DST Port: 500, 123 (IKE/IPSEC), SRC Port: Random<br>Application Layer-> None<br>Other Characteristics-> Attack rate: Flood, Packet body size: fixed 100B, 120B | ☐ สามารถตรวจจับอัตราการโจมตีได้ |

| 1. การทดสอบการป้องกัน Volumetric Attack | | | |
|---|---|---|---|
| **รูปแบบการโจมตี** | **วัตถุประสงค์** | **รายละเอียดวิธีการ** | **ผลที่ต้องการ** |
| 1.6 UDP Flood – Burst (short - 5 second duration, 30 sec interval) | เพื่อจำลองและทดสอบการป้องกันการโจมตีผ่านโปรโตคอล UDP (IPSEC) แบบการกระจาย โดยมีการสุ่มการส่งแพ็คเกตออกไปเครื่องเป้าหมายแบบกำหนดช่วงเวลาไว้เพียงสั้นๆ แต่มีการโจมตีอย่างต่อเนื่อง เพื่อทำให้มีการใช้ทรัพยากรปลายทางสูงเป็นช่วงเวลา | พารามิเตอร์ที่ใช้ทดสอบ<br>Network Layer-> SRC IP: random, DST IP: Target<br>Transport Layer-> UDP<br>Session Layer-> DST Port: 500 (IPSEC), SRC port: Random<br>Application Layer-> None<br>Other Characteristics-> Attack rate: Flood, Packet body size: fixed = 200B | ☐ สามารถตรวจจับอัตราการโจมตีได้ |
| 1.7 UDP Flood – Burst (long - 30 second duration, 60 sec interval) | เพื่อจำลองและทดสอบการป้องกันการโจมตีผ่านโปรโตคอล UDP (SSDP) แบบการกระจาย โดยมีการสุ่มการส่งแพ็คเกตออกไปเครื่องเป้าหมายแบบกำหนดช่วงเวลาไว้นานขึ้น และเพิ่มขนาดของแพ็คเกตที่ส่งให้สูงขึ้น แต่มีการโจมตีอย่างต่อเนื่อง เพื่อทำให้มีการใช้ทรัพยากรปลายทางสูงเป็นช่วงเวลา | พารามิเตอร์ที่ใช้ทดสอบ<br>Network Layer-> SRC IP: random, DST IP: Target<br>Transport Layer-> UDP<br>Session Layer-> DST Port: 1900 (SSDP), SRC port: Random<br>Application Layer-> None<br>Other Characteristics-> Attack rate: Flood, Packet body size: fixed = 250B | ☐ สามารถตรวจจับอัตราการโจมตีได้ |

| 1. การทดสอบการป้องกัน Volumetric Attack | | | |
|---|---|---|---|
| **รูปแบบการโจมตี** | **วัตถุประสงค์** | **รายละเอียดวิธีการ** | **ผลที่ต้องการ** |
| 1.8 NTP Amplification Attack | เพื่อจำลองและทดสอบการป้องกันการโจมตีผ่านโปรโตคอล NTP ที่การปลอม IP ของเครื่องต้นทาง-ปลายทางแล้วทำการ Request ออกไปยัง NTP เยอะๆ เพื่อก่อให้เกิด Response ปริมาณมากส่งกลับไปยังเครื่องเป้าหมาย | พารามิเตอร์ที่ใช้ทดสอบNetwork Layer-> SRC IP: random, DST IP: TargetTransport Layer-> UDP Session Layer-> SRC Port: 123 (NTP), DST Port: 123 (NTP)Application Layer-> None Other Characteristics-> Attack rate: Faster, Packet body size: 1400B | ☐ สามารถตรวจจับอัตราการโจมตีได้ |
| 1.9 TCP Invalid Flags Flood | เพื่อจำลองและทดสอบการป้องกันการโจมตีผ่านโปรโตคอล TCP โดยทำการส่งแพ็คเกต SYN/FIN/RST ออกไปยังเครื่องเป้าหมายจำนวนมาก เพื่อให้เกิดการเชื่อมต่อที่ไม่ถูกต้อง | พารามิเตอร์ที่ใช้ทดสอบ<br>Network Layer-> SRC IP: random, DST IP: Target<br>Transport Layer-> TCP – SYN/FIN/RST<br>Session Layer-> DST Port: 80 (HTTP)<br>Application Layer-> None<br>Other Characteristics-> Attack rate: Flood, Packet body size: 20B | ☐ สามารถตรวจจับอัตราการโจมตีได้ |

| 1. การทดสอบการป้องกัน Volumetric Attack | | | |
|---|---|---|---|
| **รูปแบบการโจมตี** | **วัตถุประสงค์** | **รายละเอียดวิธีการ** | **ผลที่ต้องการ** |
| 1.10 TCP ACK Flood | เพื่อจำลองและทดสอบการป้องกันการโจมตีผ่านโปรโตคอล TCP โดยทำการส่งแพ็คเกต ACK ออกไปยังเครื่องเป้าหมายจำนวนมาก เพื่อให้เกิดการเชื่อมต่อที่ไม่ถูกต้อง | พารามิเตอร์ที่ใช้ทดสอบ<br>Network Layer-> SRC IP: random, DST IP: Target<br>Transport Layer -> TCP – ACK<br>Session Layer -> DST Port: 80 (HTTP)<br>Application Layer-> None<br>Other Characteristics-> Attack rate: Flood, Packet body size: 20B | ☐ สามารถตรวจจับอัตราการโจมตีได้ |
| 1.11 TCP FRAG Flood | เพื่อจำลองและทดสอบการป้องกันการโจมตีผ่านโปรโตคอล TCP โดยทำการส่งแพ็คเกต RST ออกไปยังเครื่องเป้าหมายจำนวนมาก เพื่อให้เกิดการเชื่อมต่อที่ไม่ถูกต้อง | พารามิเตอร์ที่ใช้ทดสอบ<br>Network Layer-> SRC IP: random, DST IP: Target<br>Transport Layer -> TCP – RST<br>Session Layer -> SRC Port: Random, DST Port: 80 (HTTP)<br>Application Layer-> None<br>Other Characteristics-> Attack rate: Flood, Packet body size: 1800B | ☐ สามารถตรวจจับอัตราการโจมตีได้ |

| 1. การทดสอบการป้องกัน Volumetric Attack | | | |
|---|---|---|---|
| **รูปแบบการโจมตี** | **วัตถุประสงค์** | **รายละเอียดวิธีการ** | **ผลที่ต้องการ** |
| 1.12 TCP SYN/ACK Flood | เพื่อจำลองและทดสอบการป้องกันการโจมตีผ่านโปรโตคอล TCP โดยทำการส่งแพ็คเกต SYN/ACK ออกไปยังเครื่องเป้าหมายจำนวนมาก เพื่อให้เกิดการเชื่อมต่อที่ไม่ถูกต้อง | พารามิเตอร์ที่ใช้ทดสอบNetwork Layer-> SRC IP: random, DST IP: TargetTransport Layer-> TCP – SYN/ACK Session Layer -> DST Port: 80 (HTTP) Application Layer-> NoneOther Characteristics-> Attack rate: Flood, Packet body size: 500B | ☐ สามารถตรวจจับอัตราการโจมตีได้ |
| 1.13 TCP SYN Flood | เพื่อจำลองและทดสอบการป้องกันการโจมตีผ่านโปรโตคอล TCP โดยทำการส่งแพ็คเกต SYN ออกไปยังเครื่องเป้าหมายจำนวนมาก เพื่อให้เกิดการเชื่อมต่อที่ไม่ถูกต้อง | พารามิเตอร์ที่ใช้ทดสอบ<br>Network Layer-> SRC IP: random, DST IP: Target<br>Transport Layer-> TCP – SYN<br>Session Layer-> DST Port: TCP/80<br>Application Layer-> HTTP<br>Other Characteristics-> Attack rate: Flood, Packet body size: 20B | ☐ สามารถตรวจจับอัตราการโจมตีได้ |

| 1. การทดสอบการป้องกัน Volumetric Attack | | | |
|---|---|---|---|
| **รูปแบบการโจมตี** | **วัตถุประสงค์** | **รายละเอียดวิธีการ** | **ผลที่ต้องการ** |
| 1.14 ICMP Flood Attack Random Packet Size | เพื่อจำลองและทดสอบการป้องกันการโจมตีผ่านโปรโตคอล ICMP โดยทำการส่งแพ็คเก็ต ICMP ขนาดใหญ่จำนวนมากไปยังเป้าหมาย | พารามิเตอร์ที่ใช้ทดสอบ<br>Network Layer -> SRC IP: random, DST IP: Target<br>Transport Layer-> ICMP<br>Session Layer-> None<br>Application Layer-> None<br>Other Characteristics-> Attack rate: Flood, Packet body size: random < 1500B | ☐ สามารถตรวจจับอัตราการโจมตีได้ |
| 1.15 Unknown Protocol Attack | เพื่อจำลองและทดสอบการป้องกันการโจมตีผ่านโปรโตคอลที่ไม่ทราบโดยทำการสุ่มการส่งแพ็คเก็ตจำนวนมากไปยังเป้าหมาย | พารามิเตอร์ที่ใช้ทดสอบ<br>Network Layer-> SRC IP: random, DST IP: Target<br>Transport Layer-> Unknown<br>Session Layer-> None<br>Application Layer-> None<br>Other Characteristics-> Attack rate: Flood, Packet body size: none | ☐ สามารถตรวจจับอัตราการโจมตีได้ |

| 2. การทดสอบการป้องกัน Mirai Botnet Attack | | | |
|---|---|---|---|
| **รูปแบบการโจมตี** | **วัตถุประสงค์** | **รายละเอียดวิธีการ** | **ผลที่ต้องการ** |
| 2.1 Mirai: GRE Ethernet Flood | เพื่อการจำลองและทดสอบการป้องกันการโจมตีโดยใช้ Botnet โดยทำส่งแพ็คเกจ GRE ที่ห่อหุ้มข้อมูลจำนวนมากไปยังเป้าหมาย | พารามิเตอร์ที่ใช้ทดสอบNetwork Layer -> SRC IP: Attacker - Encapsulated SRC IP: Random, DST IP: Target – Encapsulated DST IP: RandomTransport Layer -> UDP Session Layer-> None Application Layer-> NoneOther Characteristics-> Attack rate: Flood, Packet body size: 512B | ☐ สามารถตรวจจับอัตราการโจมตีได้ |

| 2. การทดสอบการป้องกัน Mirai Botnet Attack | | | |
|---|---|---|---|
| **รูปแบบการโจมตี** | **วัตถุประสงค์** | **รายละเอียดวิธีการ** | **ผลที่ต้องการ** |
| 2.2 Mirai: UDP Plain Flood | เพื่อการจำลองและทดสอบการป้องกันการโจมตีโดยใช้ Botnet โดยเป็นการโจมตีผ่านโปรโตคอล UDP ซึ่งทำการการสุ่มพอร์ตต้นทางและพอร์ตปลายทาง รวมกับ IP ต้นทางที่หลากหลาย(มาจากบ็อตหลายตัว) เพื่อส่งแพ็คเกตไปยังเป้าหมาย | พารามิเตอร์ที่ใช้ทดสอบ<br>Network Layer-> SRC IP: Attacker, DST IP: Target<br>Transport Layer-> UDP<br>Session Layer-> None<br>Application Layer-> None<br>Other Characteristics Attack rate: Flood, Packet body size: 512B | ☐ สามารถตรวจจับอัตราการโจมตีได้ |
| 2.3 Mirai: HTTP Flood | เพื่อการจำลองและทดสอบการป้องกันการโจมตีโดยใช้ Botnet โดยเป็นการโจมตีผ่านโปรโตคอล HTTP โดยการส่งชุดคำขอ GET หรือ POST จำนวนมากไปยังเป้าหมาย | พารามิเตอร์ที่ใช้ทดสอบ<br>Network Layer-> SRC IP: Attacker, DST IP: Target<br>Transport Layer-> TCP<br>Session Layer-> None<br>Application Layer-> HTTP<br>Other Characteristics-> Attack rate: Flood, Packet body size: 512B | ☐ สามารถตรวจจับอัตราการโจมตีได้ |

| 2. การทดสอบการป้องกัน Mirai Botnet Attack | | | |
|---|---|---|---|
| **รูปแบบการโจมตี** | **วัตถุประสงค์** | **รายละเอียดวิธีการ** | **ผลที่ต้องการ** |
| 2.4 Mirai: GRE IP Flood | เพื่อการจำลองและทดสอบการป้องกันการโจมตีโดยใช้ Botnet โดยเป็นการโจมตีผ่านโปรโตคอล TCP ซึ่งทำการการสุ่มพอร์ตต้นทางและพอร์ตปลายทาง รวมกับ IP ต้นทางที่หลากหลาย(มาจากบ็อตหลายตัว) เพื่อส่งแพ็คเกตไปยังเป้าหมาย | พารามิเตอร์ที่ใช้ทดสอบ<br>Network Layer-> SRC IP: Attacker - Encapsulated SRC IP: Random, DST IP: Target – Encapsulated DST IP: Random<br>Transport Layer-> UDP<br>Session Layer-> None<br>Application Layer-> None<br>Other Characteristics-> Attack rate: Flood, Packet body size: 512B | ☐ สามารถตรวจจับอัตราการโจมตีได้ |
| 2.5 Mirai: UDP Flood | เพื่อการจำลองและทดสอบการป้องกันการโจมตีโดยใช้ Botnet โจมตีผ่านโปรโตคอล UDP พร้อมทั้งมีการสุ่ม IP ต้นทาง-ปลายทาง สุ่ม Port การเชื่อมต่อทั้งปลายทางและต้นทาง สุ่มขนาดของแพ็ตเกตในการโจมตี | พารามิเตอร์ที่ใช้ทดสอบNetwork Layer-> SRC IP: Attacker, DST IP: TargetTransport Layer-> UDP Session Layer-> None Application Layer-> NoneOther Characteristics-> Attack rate: Flood, Packet body size: 512B | ☐ สามารถตรวจจับอัตราการโจมตีได้ |

| 2. การทดสอบการป้องกัน Mirai Botnet Attack | | | |
|---|---|---|---|
| **รูปแบบการโจมตี** | **วัตถุประสงค์** | **รายละเอียดวิธีการ** | **ผลที่ต้องการ** |
| 2.6 Mirai: VSE Flood | เพื่อการจำลองและทดสอบการป้องกันการโจมตีโดยใช้ Botnet โดยทำการส่งแพ็คเกจไปยัง port ของเครื่องปลายทางที่เปิดไว้เฉพาะส่วนใหญ่มักเจอในการโจมตีเกมส์ต่าง | พารามิเตอร์ที่ใช้ทดสอบ<br>Network Layer-> SRC IP: Attacker, DST IP: Target<br>Transport Layer-> TCP<br>Session Layer-> None<br>Application Layer-> UDP/27015<br>Other Characteristics-> Attack rate: Flood, Packet body size: 25B | ☐ สามารถตรวจจับอัตราการโจมตีได้ |
| 2.7 Mirai: DNS Waterfall Flood | เพื่อการจำลองและทดสอบการป้องกันการโจมตีโดยใช้ Botnet โจมตีผ่าน DNS เพื่อทำการปลอม IP ของเครื่องต้นทาง-ปลายทาง แล้วทำการ Request ออกไปยัง NTP เยอะๆ เพื่องก่อให้เกิด Response ปริมาณมากส่งกลับไปยังเครื่องเป้าหมาย | พารามิเตอร์ที่ใช้ทดสอบ<br>Network Layer-> SRC IP: Attacker, DST IP: Target<br>Transport Layer-> UDP<br>Session Layer-> None<br>Application Layer-> DNS<br>Other Characteristics-> Attack rate: Flood, Packet body size: 43B | ☐ สามารถตรวจจับอัตราการโจมตีได้ |

| 2. การทดสอบการป้องกัน Mirai Botnet Attack | | | |
|---|---|---|---|
| **รูปแบบการโจมตี** | **วัตถุประสงค์** | **รายละเอียดวิธีการ** | **ผลที่ต้องการ** |
| 2.8 Mirai: SYN Flood | เพื่อการจำลองและทดสอบการป้องกันการโจมตีโดยใช้ Botnet ส่งแพ็คเกต SYN ออกไปยังเครื่องเป้าหมายจำนวนมาก(จาก Botnet หลายตัว) เพื่อให้เกิดการเชื่อมต่อที่ไม่ถูกต้อง | พารามิเตอร์ที่ใช้ทดสอบ<br>Network Layer-> SRC IP: Attacker, DST IP: Target<br>Transport Layer-> TCP<br>Session Layer-> None<br>Application Layer-> HTTP<br>Other Characteristics-> Attack rate: Flood, Packet body size: 20B | ☐ สามารถตรวจจับอัตราการโจมตีได้ |
| 2.9 Mirai: ACK Flood | เพื่อการจำลองและทดสอบการป้องกันการโจมตีโดยใช้ Botnet ส่งแพ็คเกต ACK ออกไปยังเครื่องเป้าหมายจำนวนมาก(จาก Botnet หลายตัว) เพื่อให้เกิดการเชื่อมต่อที่ไม่ถูกต้อง | พารามิเตอร์ที่ใช้ทดสอบNetwork Layer-> SRC IP: Attacker, DST IP: TargetTransport Layer-> TCP Session Layer-> None Application Layer-> NoneOther Characteristics-> Attack rate: Flood, Packet body size: 512B | ☐ สามารถตรวจจับอัตราการโจมตีได้ |

| 2. การทดสอบการป้องกัน Mirai Botnet Attack | | | |
|---|---|---|---|
| **รูปแบบการโจมตี** | **วัตถุประสงค์** | **รายละเอียดวิธีการ** | **ผลที่ต้องการ** |
| 2.10 Mirai: STOMP Flood | เพื่อการจำลองและทดสอบการป้องกันการโจมตีโดยใช้ Botnet โดยใช้วิธี STOMP Flood ในการโจมตีเครื่องเป้าหมาย | พารามิเตอร์ที่ใช้ทดสอบ<br>Network Layer-> SRC IP: Attacker, DST IP: Target<br>Transport Layer-> TCP<br>Session Layer-> None<br>Application Layer-> HTTP<br>Other Characteristics-> Attack rate: Flood, Packet body size: 32B | ☐ สามารถตรวจจับอัตราการโจมตีได้ |

| 3. การทดสอบการป้องกัน Application DDOS Attack | | | |
|---|---|---|---|
| **รูปแบบการโจมตี** | **วัตถุประสงค์** | **รายละเอียดวิธีการ** | **ผลที่ต้องการ** |
| 3.1 DNS Query Flood | เพื่อจำลองและทดสอบการป้องกันการโจมตีผ่าน Application ที่เขียนขึ้นมาทำการโจมตี DNS เพื่อทำการปลอม IP ของเครื่องต้นทาง-ปลายทางแล้วทำการ Request ออกไปยัง DNS มากๆ เพื่อก่อให้เกิด Response ปริมาณมากส่งกลับไปยังเครื่องเป้าหมาย | พารามิเตอร์ที่ใช้ทดสอบ<br>Network Layer-> SRC IP: random, DST IP: Target<br>Transport Layer-> UDP<br>Session Layer-> DST Port: 53 (DNS), SRC Port: Random<br>Application Layer-> DNS Query<br>Other Characteristics-> Attack rate: Flood, Packet body size: fixed | ☐ สามารถตรวจจับอัตราการโจมตีได้ |
| 3.2 DNS Waterfall (Pseudo Random Query Flood) | เพื่อจำลองและทดสอบการป้องกันการโจมตีผ่าน Application ที่เขียนขึ้นมาทำการโจมตี DNS คือทำการร้องขอที่อยู่ IP ของ โดเมน รวมไปถึงโดเมนที่อยู่ภายใต้โดเมนหลักด้วย เพื่อทำการปลอม IP ของเครื่องต้นทาง-ปลายทางแล้วทำการ Request ออกไปยัง DNS มากๆ เพื่อก่อให้เกิด Response ปริมาณมากส่งกลับไปยังเครื่องเป้าหมาย | พารามิเตอร์ที่ใช้ทดสอบ<br>Network Layer-> SRC IP: random DST IP: Target<br>Transport Layer-> UDP<br>Session Layer-> DST Port: 53 (DNS), SRC Port: Random<br>Application Layer-> DNS Query<br>Other Characteristics-> Attack rate: Flood, Packet body size: random | ☐ สามารถตรวจจับอัตราการโจมตีได้ |

| 3. การทดสอบการป้องกัน Application DDOS Attack | | | |
|---|---|---|---|
| **รูปแบบการโจมตี** | **วัตถุประสงค์** | **รายละเอียดวิธีการ** | **ผลที่ต้องการ** |
| 3.3 DNS Query Flood (NonExisting (NX) Domain) | เพื่อจำลองและทดสอบการป้องกันการโจมตีผ่าน Application ที่เขียนขึ้นมาทำการโจมตี DNS คือ ทำการร้องขอที่อยู่ IP ของ โดเมน รวมไปถึงโดเมนที่อยู่ภายใต้โดเมนหลักด้วย เพื่อทำการปลอม Request ออกไปยัง DNS มากๆ เพื่อก่อให้เกิดการจัดการปริมาณ Request มากๆ | พารามิเตอร์ที่ใช้ทดสอบNetwork Layer-> SRC IP: random, DST IP: Target Transport Layer-> UDP Session Layer-> DST Port: 53 (DNS), SRC Port: RandomApplication Layer-> DNS Query Other Characteristics-> Attack rate: Flood, Packet body size: random | ☐ สามารถตรวจจับอัตราการโจมตีได้ |
| 3.4 DNS Invalid Payload (non RFC Compliant) | เพื่อจำลองและทดสอบการป้องกันการโจมตีผ่าน Application ที่เขียนขึ้นมาโดยใช้การโจมตีแบบ DNS Invalid Payload (non RFC Compliant) | พารามิเตอร์ที่ใช้ทดสอบ<br>Network Layer-> SRC IP: random, DST IP: Target<br>Transport Layer-> UDP<br>Session Layer-> DST Port: 53 (DNS) SRC Port: Random<br>Application Layer->DNS Query<br>Other Characteristics-> Attack rate: Flood, Packet body size: random | ☐ สามารถตรวจจับอัตราการโจมตีได้ |

| 3. การทดสอบการป้องกัน Application DDOS Attack | | | |
|---|---|---|---|
| **รูปแบบการโจมตี** | **วัตถุประสงค์** | **รายละเอียดวิธีการ** | **ผลที่ต้องการ** |
| 3.5 DNS Reflection Flood | เพื่อจำลองและทดสอบการป้องกันการโจมตีผ่าน Application ที่เขียนขึ้นมาโดยใช้การโจมตีแบบ DNS Reflection Flood | พารามิเตอร์ที่ใช้ทดสอบ<br>Network Layer-> SRC IP: random, DST IP: Target<br>Transport Layer-> UDP<br>Session Layer-> DST Port: Random SRC Port: 53<br>Application Layer-> DNS Query<br>Other Characteristics-> Attack rate: Flood, Packet body size: random | ☐ สามารถตรวจจับอัตราการโจมตีได้ |
| 3.6 HTTP GET Flood – High CPS (Connection Per Second) | เพื่อจำลองและทดสอบการป้องกันการโจมตีผ่าน Application ที่เขียนขึ้นมาโดยใช้การโจมตีแบบ HTTP GET Flood – High CPS (Connection Per Second) | พารามิเตอร์ที่ใช้ทดสอบ<br>Network Layer-> SRC IP: random from pool, DST IP: Target<br>Transport Layer-> TCP<br>Session Layer-> DST Port: 80 (HTTP) SRC Port: Random<br>Application Layer-> HTTP<br>Other Characteristics-> Attack rate: Flood, Packet body size: random | ☐ สามารถตรวจจับอัตราการโจมตีได้ |

| 3. การทดสอบการป้องกัน Application DDOS Attack | | | |
|---|---|---|---|
| **รูปแบบการโจมตี** | **วัตถุประสงค์** | **รายละเอียดวิธีการ** | **ผลที่ต้องการ** |
| 3.7 HTTP GET Flood – High RPS (Request Per Second) | เพื่อจำลองและทดสอบการป้องกันการโจมตีผ่าน Application ที่เขียนขึ้นมาโดยใช้การโจมตีแบบ HTTP GET Flood – High RPS (Request Per Second) | พารามิเตอร์ที่ใช้ทดสอบNetwork Layer-> SRC IP: random from pool, DST IP: Target Transport Layer-> TCP Session Layer-> DST Port: 80 (HTTP) SRC Port: Random Application Layer-> HTTP Other Characteristics-> Attack rate: Flood, Packet body size: random | ☐ สามารถตรวจจับอัตราการโจมตีได้ |
| 3.8 HTTPs GET Flood – High CPS (Connection Per Second) | เพื่อจำลองและทดสอบการป้องกันการโจมตีผ่าน Application ที่เขียนขึ้นมาโดยใช้การโจมตีแบบ HTTPs GET Flood – High CPS (Connection Per Second) | พารามิเตอร์ที่ใช้ทดสอบ<br>Network Layer-> SRC IP: Attacker, DST IP: Target<br>Transport Layer-> TCP<br>Session Layer-> DST Port: 443 (HTTPS), SRC Port: Random<br>Application Layer-> HTTPS Requests<br>Other Characteristics-> Attack rate: Flood, Packet body size: Fixed Payloads | ☐ สามารถตรวจจับอัตราการโจมตีได้ |

| 3. การทดสอบการป้องกัน Application DDOS Attack | | | |
|---|---|---|---|
| **รูปแบบการโจมตี** | **วัตถุประสงค์** | **รายละเอียดวิธีการ** | **ผลที่ต้องการ** |
| 3.9 HTTPs GET Flood - High RPS (Request Per Second) | เพื่อจำลองและทดสอบการป้องกันการโจมตีผ่าน Application ที่เขียนขึ้นมาโดยใช้การโจมตีแบบ HTTPs GET Flood - High RPS (Request Per Second) | พารามิเตอร์ที่ใช้ทดสอบ<br>Network Layer-> SRC IP: Attacker, DST IP: Target<br>Transport Layer-> TCP<br>Session Layer-> DST Port: 443 (HTTPS), SRC Port: Random<br>Application Layer-> HTTPS Requests<br>Other Characteristics-> Attack rate: Flood, Packet body size: random | ☐ สามารถตรวจจับอัตราการโจมตีได้ |