การแข่งขันป้องกันทางไซเบอร์ Cyber Defence Exercise (CDX) 2016

ในงานสัปดาห์วิชาการความมั่นคง สถาบันวิชาการป้องกันประเทศ ๒๕๕๙ NDSI Security Week 2016 ๑๑-๑๓ พฤษภาคม ๒๕๕๙

บทความพิเศษ

กองบรรณสารและเทคโนโลยีสารสนเทศ
กองบัญชาการสถาบันวิชาการป้องกันประเทศ

การแข่งขันในรูปแบบของ Cyber Defence ที่ยิ่งใหญ่ที่สุดในระดับหน่วยงานความมั่นคงของภาครัฐ รัฐวิสาหกิจ และสถาบันการศึกษาของประเทศไทย เพื่อค้นหาสุดยอดฝีมือนักรบไซเบอร์ (Cyber Warrior) ในระดับประเทศ ณ สถาบันวิชาการป้องกันประเทศ

ความเป็นมา

สถาบันวิชาการป้องกันประเทศ มีพันธกิจในงานด้านวิชาการและการศึกษาด้านความมั่นคงแห่งชาติ ยุทธศาสตร์และวิทยาการทหาร โดยในปัจจุบันภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber security) ได้ทวีความรุนแรงเพิ่มมากยิ่งขึ้น ในขณะที่บุคลากรที่มีความรู้ ทักษะและความเชี่ยวชาญยังคงมีจำกัด ซึ่งควรเร่งพัฒนาศักยภาพ และเสริมสร้างทักษะ ประสบการณ์ด้านความปลอดภัยไซเบอร์ให้แก่บุคลากร/ข้าราชการของรัฐ รัฐวิสาหกิจ ที่มีหน้าที่รับผิดชอบในระบบสารสนเทศที่สำคัญ ซึ่งรวมถึงนิสิต นักศึกษา อันจะเป็นกำลังสำคัญในอนาคตของประเทศชาติ

สถาบันวิชาการป้องกันประเทศได้จัดการแข่งขันป้องกันการโจมตีทางไซเบอร์โดยระบบจำลองยุทธ์ Cyber W.A.R. หรือ Cyber Defence Exercise (CDX) 2016 มาอย่างต่อเนื่อง โดยกิจกรรมครั้งแรก จัดขึ้นเมื่อวันพุธที่ ๖ พฤษภาคม ๒๕๕๗ โดยในครั้งนั้น มีผู้ให้ความสนใจสมัครเข้าร่วมการแข่งขันทั้งสิ้น ๑๒ ทีม โดยผ่านเข้าสู่การแข่งขันรอบคัดเลือกจำนวน ๘ ทีม และทีมที่ชนะเลิศ ได้แก่ ทีม Pwnladin ซึ่งมีสมาชิกเป็นนักศึกษาจากมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี ร่วมกับมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

เพื่อให้การส่งเสริม และพัฒนาทักษะด้านความมั่นคงปลอดภัยไซเบอร์เกิดขึ้นอย่างต่อเนื่อง สถาบันวิชาการป้องกันประเทศ จึงจัดการแข่งขันป้องกันการโจมตีทางไซเบอร์ หรือ Cyber Defence Exercise (CDX) 2016 ขึ้นอีกครั้งภายในงานสัปดาห์วิชาการความมั่นคง สถาบันวิชาการป้องกันประเทศ ๒๕๕๙ (NDSI Security Week 2016) ระหว่างวันที่ ๑๑-๑๓ พฤษภาคม ๒๕๕๙

รูปที่ ๑ การแข่งขันป้องกันทางไซเบอร์ (Cyber Defence Exercise) ในการประชุมสัมมนาไซเบอร์แห่งชาติ ในงานสัปดาห์วิชาการความมั่นคงของสถาบันวิชาการป้องกันประเทศ National Cyber Security Conference @ National Defence Studies Institute Security Week 2014 ณ ห้องบรรยายรวมวิทยาลัยป้องกันราชอาณาจักร สถาบันวิชาการป้องกันประเทศ ถนนวิภาวดีรังสิต กรุงเทพมหานคร เมื่อวันพุธที่ ๖ – วันพฤหัสบดีที่ ๗ พฤษภาคม ๒๕๕๗

วัตถุประสงค์

๑. เพื่อทดสอบความรู้และประสบการณ์ในการแก้ปัญหาจากการโจมตีทางไซเบอร์ (Cyber Attack) ของหน่วยงานด้านความมั่นคงของภาครัฐ รัฐวิสาหกิจ และสถาบันการศึกษา

๒. เพื่อขยายฐานความรู้ ทักษะ และพัฒนาการของบุคลากรภายในหน่วยงานความมั่นคงของภาครัฐ รัฐวิสาหกิจ และสถาบันการศึกษา ให้มีส่วนร่วมในการตั้งรับ และป้องกันการโจมตีทางไซเบอร์ รวมถึงการฟื้นฟูระบบสารสนเทศของหน่วยงานอย่างเป็นรูปธรรม

๓. เพื่อค้นหาผู้เชี่ยวชาญด้าน Cyber Warfare ทั้งเชิงรุกและเชิงรับ

กลุ่มเป้าหมาย และคุณสมบัติของผู้เข้าร่วมการแข่งขัน

โครงการแข่งขันป้องกันการโจมตีทางไซเบอร์ โดยระบบจำลองยุทธ์ Cyber W.A.R. ประจำปี ๒๕๕๙ หรือ Cyber Defence Exercise (CDX) 2016 จัดขึ้นเป็นครั้งที่ ๒ ซึ่งกำหนดกลุ่มบุคคลเป้าหมายที่จะสามารถสมัครเข้าร่วมการแข่งขัน ดังนี้

๑. นิสิตนักศึกษา(ระดับปริญญาตรีหรือปริญญาโท)

๒. พนักงานรัฐวิสาหกิจ

๓. ข้าราชการพลเรือน

๔. ข้าราชการทหาร หรือข้าราชการซึ่งปฏิบัติหน้าที่ด้านความมั่นคง

ทั้งนี้ จะได้ดำเนินการเปิดรับสมัครให้เข้าร่วมการแข่งขันในรูปแบบทีม โดยมีสมาชิกสูงสุดทีมละไม่เกิน ๓ ท่าน โดยจำเป็นต้องมีความรู้ และทักษะด้านระบบปฏิบัติการระบบเครือข่าย และการรักษาความปลอดภัยสารสนเทศ ดังนี้

๑. ความรู้พื้นฐานทางด้าน Network, TCP/IP, OS

๒. การใช้งานคำสั่ง (Command) ของระบบปฏิบัติการ UNIX, Linux, Windows

๓. ความรู้ในเรื่องของ Common Vulnerabilities and Exposures (CVE)

๔. การใช้เครื่องมือ (ICT Security Tools) ต่างๆ ในเชิงรุก และเชิงรับ ได้เป็นอย่างดี เช่น BACKTRACK, TCP DUMP และ nMAP เป็นต้น

กำหนดการ

เพื่อให้การดำเนินงานโครงการแข่งขันป้องกันการโจมตีทางไซเบอร์ในครั้งนี้บรรลุตามวัตถุประสงค์ คณะดำเนินงานจึงได้กำหนด (ร่าง) กำหนดการสำหรับกิจกรรมต่าง ๆ ไว้ ดังนี้

๑-๒๒ เมษายน ๕๙ ประชาสัมพันธ์ และรับสมัคร (ออนไลน์) https://goo.gl/d32bnD

๒๗ เมษายน ๕๙ ประกาศรายชื่อผู้ที่ผ่านการตรวจสอบคุณสมบัติ และรับรองให้เข้าร่วมการแข่งขัน

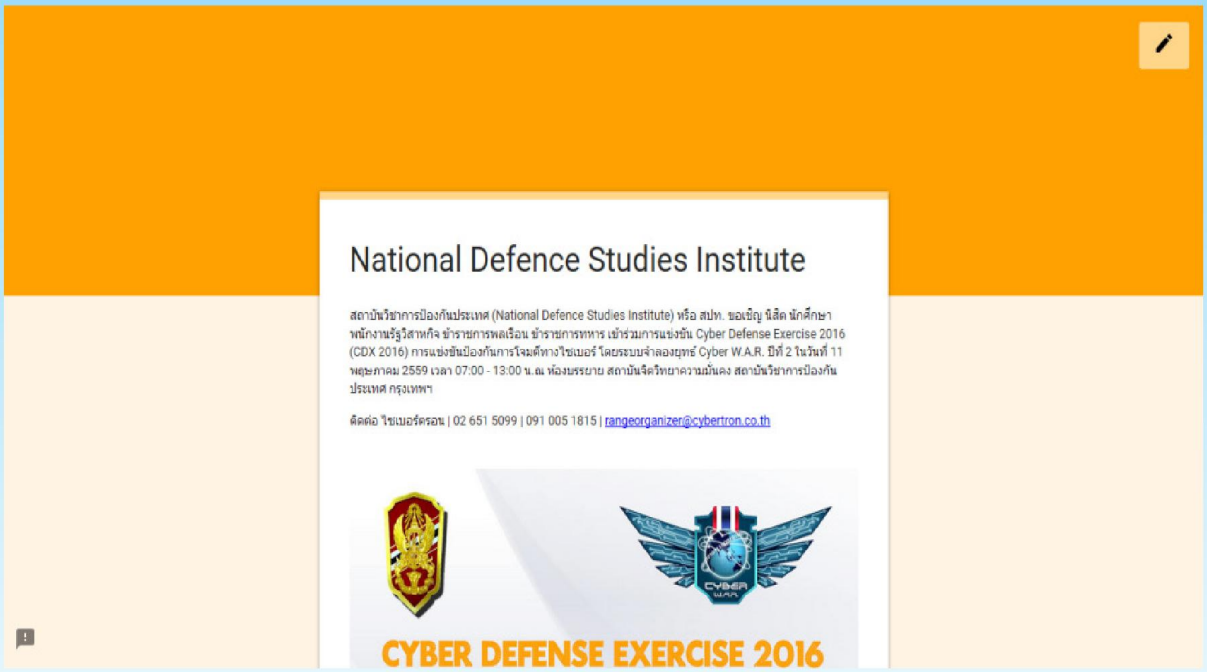
๒๙ เมษายน ๕๙ การประเมินความรู้พื้นฐานด้วยแบบทดสอบ (รอบคัดเลือก)

๓ พฤษภาคม ๕๙ ประกาศรายชื่อทีมที่ได้รับการคัดเลือกให้เข้าสู่การแข่งขันรอบชิงชนะเลิศ

๑๑ พฤษภาคม ๕๙ การแข่งขัน CDX 2016 รอบชิงชนะเลิศ

การลงทะเบียนสมัครเข้าแข่งขัน

ผู้ที่มีความสนใจ และประสงค์จะสมัครเข้าร่วมการแข่งขัน สามารถบันทึกข้อมูลเบื้องต้นได้ที่ https://goo.gl/d32bnD ซึ่งเมื่อบันทึกข้อมูลเบื้องต้นเป็นที่เรียบร้อยแล้ว เจ้าหน้าที่ของคณะดำเนินงานจะได้ติดต่อกลับไปยังผู้สมัครเพื่อตรวจสอบข้อมูลการสมัคร และดำเนินการตามขั้นตอนการรับสมัครต่อไป



รูปที่ ๒ แบบฟอร์มการลงทะเบียนรับสมัครผู้เข้าแข่งขัน

การตรวจสอบคุณสมบัติของผู้เข้าร่วมการแข่งขัน

เมื่อผู้สมัครได้ลงทะเบียนเข้าร่วมการแข่งขันโดยกรอกข้อมูลสำคัญผ่านแบบฟอร์มรับลงทะเบียนเป็นที่เรียบร้อยแล้ว คณะดำเนินงานจะได้รวบรวมข้อมูล และตรวจสอบย้อนกลับไปยังผู้บันทึกข้อมูลเพื่อสอบถามความเข้าใจเกี่ยวกับสถานะของผู้ลงทะเบียนเข้าร่วมการแข่งขัน จากนั้น จะได้ดำเนินการตรวจสอบกับบุคคลผู้อ้างอิง (Reference Person) เพื่อให้ความเห็นเกี่ยวกับสถานะ และทัศนคติของผู้ลงทะเบียน เพื่อรวบรวมและนำเสนอต่อสถาบันวิชาการป้องกันประเทศพิจารณาอนุมัติรายชื่อผู้เข้าร่วมการแข่งขันต่อไป

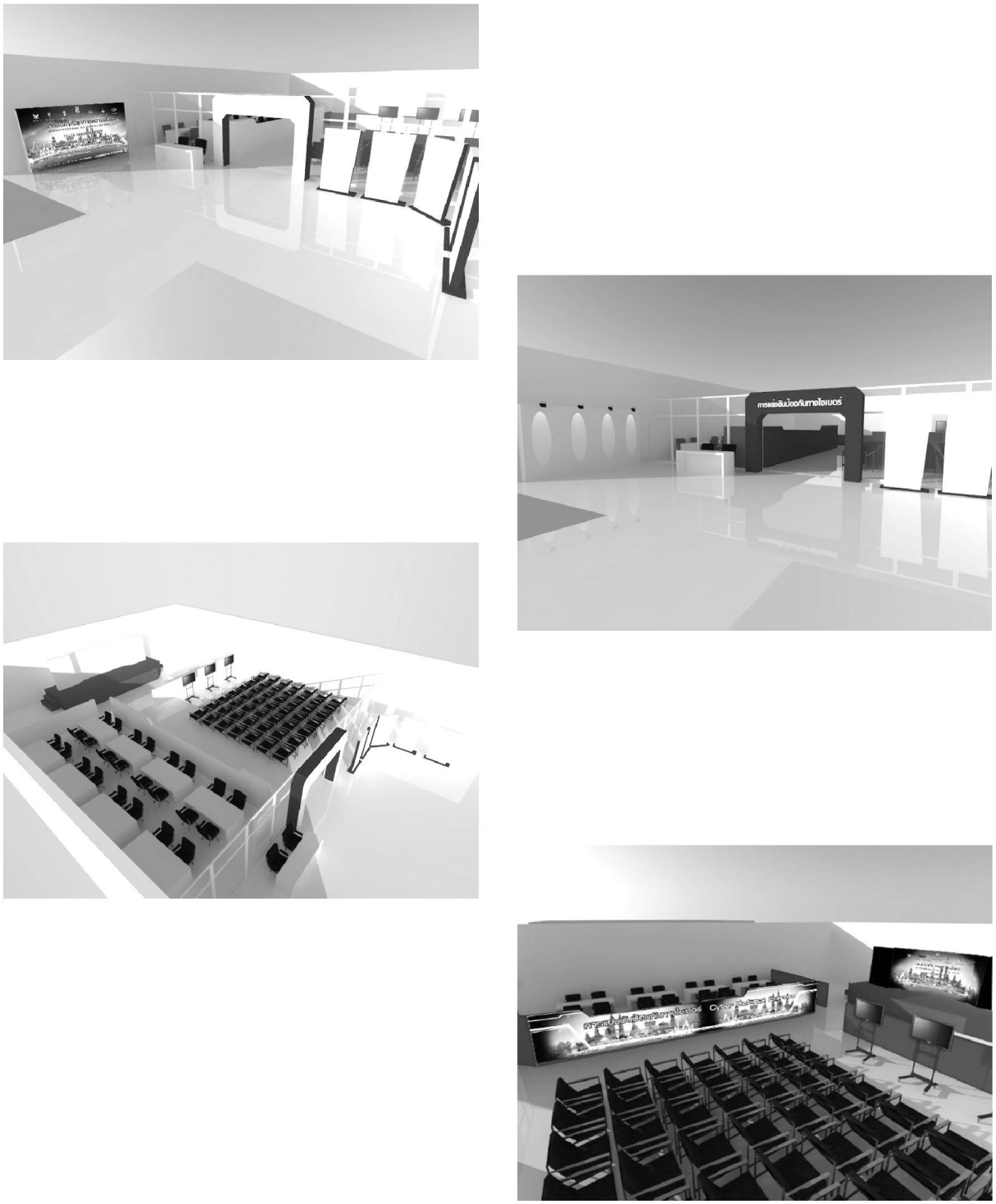
เมื่อสถาบันวิชาการป้องกันประเทศได้พิจารณารับรองรายชื่อผู้ลงทะเบียนเข้าร่วมการแข่งขันแล้ว และได้ประกาศรายชื่อทีมที่ผ่านการรับรองคุณสมบัติ จึงจะส่งเข้าสู่กระบวนการคัดเลือกผู้เข้าแข่งขันตามขั้นตอนต่อไป

การประเมินความรู้พื้นฐานด้วยแบบทดสอบ (รอบคัดเลือก)

ผู้ลงทะเบียนเข้าร่วมการแข่งขันและได้รับการรับรองรายชื่อแล้ว จะต้องจัดกลุ่มร่วมกันและดำเนินการทำแบบทดสอบเพื่อประเมินพื้นฐานความรู้ ด้วยแบบทดสอบแบบปรนัย จำนวน ๕๐ ข้อ ซึ่งมีเนื้อหาครอบคลุมความรู้พื้นฐานตามที่กำหนด ทั้งนี้ คณะผู้ดำเนินงานจะได้จัดทำแบบทดสอบในรูปแบบเอกสาร หรือรูปแบบออนไลน์ (Web-Based) โดยที่ผู้ลงทะเบียนเข้าร่วมการแข่งขันจะต้องส่งคำตอบให้ทันตามกำหนดเวลา ซึ่งจะได้แจ้งรายละเอียดให้ทราบในขั้นตอนการประเมินความรู้พื้นฐาน

อนึ่ง ในการประเมินความรู้พื้นฐานนี้ ผู้สมัครควรศึกษาแบบทดสอบและหารือเฉพาะภายในทีมของตนเอง เพื่อให้ได้คำตอบที่ดีที่สุด โดยไม่ควรพึ่งการสอบถามบุคคลอื่นที่ไม่เกี่ยวข้อง หรือค้นหาข้อมูลจากทั้งจากตำราหรืออินเทอร์เน็ต และควรทำแบบทดสอบให้แล้วเสร็จภายในเวลา ๓ ชั่วโมง

ผลลัพธ์จากการประเมินจะได้ถูกนำมาจัดลำดับเพื่อพิจารณาเลือก ๘ ทีมสุดท้าย ที่จะได้รับการคัดเลือกให้เข้าสู่การแข่งขันรอบชิงชนะเลิศ และจะได้จัดทีมสำรองไว้อย่างน้อย ๒ ทีม สำหรับในกรณีที่ผู้เข้าแข่งขันไม่สามารถเข้าร่วมการแข่งขันได้ ซึ่งจะได้ประกาศรายชื่อผู้ที่ผ่านการคัดเลือกให้เข้าสู่การแข่งขันรอบชิงชนะเลิศต่อไป



รูปที่ ๓ ภาพจำลองห้องการแข่งขันป้องกันทางไซเบอร์

กำหนดการรอบชิงชนะเลิศ

การแข่งขันป้องกันทางไซเบอร์ (Cyber Defence Exercise) ประจำปี พ.ศ. ๒๕๕๙ (2016) รอบชิงชนะเลิศได้จัดขึ้นควบคู่กับงานเสวนาทางวิชาการ เรื่อง "การปฏิบัติการข่าวสารกับความมั่นคง ASEAN" ณ สถาบันจิตวิทยาความมั่นคง สถาบันวิชาการป้องกันประเทศในวันพุธที่ ๑๑ พฤษภาคม ๒๕๕๙

ในการแข่งขันรอบชิงชนะเลิศ คณะดำเนินงานจะได้จัดให้มีระบบจำลองยุทธ์ทางไซเบอร์ (Warrior Attack Range) ซึ่งเป็นการจำลองทรัพยากรของระบบออกมาเป็นเครื่องคอมพิวเตอร์แม่ข่าย (Server) ซึ่งมอบหมายให้ผู้เข้าแข่งขันแต่ละทีมเป็นผู้รับผิดชอบทรัพยากรเหล่านั้น โดยการต่อเชื่อมเครื่องคอมพิวเตอร์ หรือโน้ตบุ๊กของตนเองเข้าสู่ระบบดังกล่าว และทำการค้นหาช่องโหว่ (vulnerabilities) ที่อาจมีในระบบของตนเอง และดำเนินการแก้ไข/ป้องกันมิให้ผู้เข้าแข่งขันรายอื่นเข้ามาโจมตีและยึดครองทรัพยากรเหล่านั้นได้

และในขณะเดียวกัน ผู้เข้าแข่งขันก็ต้องดำเนินการสำรวจไปยังทรัพยากรของผู้เข้าแข่งขันทีมอื่น พยายามค้นหาช่องโหว่ในระบบเหล่านั้น และพยายามยึดครองทรัพยากรของคู่แข่งขันให้ได้

ระบบจำลองยุทธ์ทางไซเบอร์ จะคำนวณคะแนนให้แต่ละทีมตามความสามารถที่ปฏิบัติได้ โดยจะได้รับคะแนนเพิ่ม ๑๐ คะแนน สำหรับทุกช่องโหว่ที่ค้นพบและสามารถยึดครองได้ หรือคะแนนหักลบ ๔๐ คะแนน เมื่อทรัพยากรในความรับผิดชอบถูกคู่แข่งขันทีมอื่นยึดครอง

กติกาการแข่งขัน

ผู้สมัครเข้าร่วมการแข่งขันที่ผ่านการคัดเลือกให้ผ่านเข้าสู่การแข่งขันรอบชิงชนะเลิศ จะต้องจัดเตรียมเครื่องคอมพิวเตอร์ และอุปกรณ์อันจำเป็นเพื่อใช้ในการแข่งขัน โดยติดตั้งระบบปฏิบัติการซึ่งสามารถเชื่อมต่อเข้าสู่เครือข่าย (Wired Network) และติดตั้งโปรแกรม (เครื่องมือ) ที่จำเป็นต่อการแข่งขันให้พร้อมก่อนเข้าสู่การแข่งขัน คณะดำเนินงานใคร่ขอเสนอกติกาการแข่งขัน (Rule of Engagement) เพื่อให้ผู้เข้าแข่งขันทุกท่านได้ถือปฏิบัติโดยเคร่งครัด ดังนี้

๑. ห้ามก่อกวนผู้อื่นโดยวิธีการ เช่น DoS, MITM, Exploitation

๒. ห้ามเปลี่ยน Password ของทุก Account ในระบบทั้งของตนเองและของทีมอื่น

๓. ห้ามปิดช่องโหว่ด้วยวิธีการปิด Service, ลบ File หรือ Parameter ใดๆ ทั้งสิ้น

๔. ห้ามเจาะระบบและโจมตีระบบอื่นใดที่อยู่นอกเหนือจากเป้าหมาย

๕. แต่ละทีมสามารถใช้ Software ประเภท Vulnerability Scanner ได้เพียงทีมละ ๑ คนเท่านั้น

๖. ห้ามผู้เข้าแข่งขันติดต่อสื่อสารกับผู้เล่นทีมอื่นระหว่างการแข่งขัน

๗. ผู้เข้าแข่งขันสามารถออกจากสนามแข่งขันได้ทีละ ๑ คนเท่านั้น โดยแจ้งเจ้าหน้าที่ควบคุมการแข่งขัน

๘. หากผู้เข้าแข่งขันต้องการออกไปด้านนอกสนามแข่งขันจะต้องมีเจ้าหน้าที่ติดตามไปด้วย

๙. การใช้งาน Internet สามารถใช้ได้ภายใต้การอนุญาตจากกรรมการเท่านั้น

๑๐. การใช้งาน Internet ของผู้เข้าแข่งขันนั้น ผู้เข้าแข่งขันจะต้องเตรียมอุปกรณ์มาเอง

๑๑. ในระหว่างการแข่งขันห้ามบุคคลอื่นเชื่อมต่อจากภายนอกเข้าสู่คอมพิวเตอร์ที่ใช้ในการแข่งขันไม่ว่ากรณีใด ๆ

๑๒. คณะกรรมการขอสงวนสิทธิ์ในการเปลี่ยนแปลงเงื่อนไข และกติกาตามความเหมาะสม

ผู้เข้าแข่งขันยินยอมปฏิบัติตามกติกาที่ระบุไว้ข้างต้นทุกประการ และผลการตัดสินของคณะกรรมการถือเป็นที่สิ้นสุด ในกรณีที่ผู้เข้าแข่งขันฝ่าฝืนกติกา ทีมของท่านจะถูกปรับแพ้ และต้องออกจากการแข่งขันโดยทันที

การประกาศผล และรางวัล

เมื่อสิ้นสุดการแข่งขันรอบชิงชนะเลิศแล้ว คณะดำเนินงานจะได้ตรวจสอบข้อมูลผลการแข่งขัน และจะได้ประกาศรับรองผลการแข่งขัน พร้อมทั้งมอบรางวัลให้แก่ทีมผู้ชนะเลิศ ซึ่งสถาบันวิชาการป้องกันประเทศได้จัดเตรียมรางวัลสำหรับผู้เข้าแข่งขันซึ่งสามารถผ่านเข้าสู่การแข่งขันรอบชิงชนะเลิศ ซึ่งได้รับคะแนนอันดับสูงสุด จำนวน ๓ อันดับแรก ซึ่งปฏิบัติตามกติกาการแข่งขันอย่างเคร่งครัด ดังนี้

รางวัลอันดับที่ ๑

รับโล่เกียรติยศ จากผู้บัญชาการสถาบันวิชาการป้องกันประเทศ พร้อมเงินรางวัล ๓๐,๐๐๐ บาท

รางวัลอันดับที่ ๒

รับโล่เกียรติยศ จากผู้บัญชาการสถาบันวิชาการป้องกันประเทศ พร้อมเงินรางวัล ๒๐,๐๐๐ บาท

รางวัลอันดับที่ ๓

รับโล่เกียรติยศ จากผู้บัญชาการสถาบันวิชาการป้องกันประเทศ พร้อมเงินรางวัล ๑๐,๐๐๐ บาท

นอกจากนี้ ผู้เข้าแข่งขันทุกท่านที่ผ่านเข้าสู่การแข่งขันรอบชิงชนะเลิศจะได้รับเกียรติบัตรทุกท่าน