<u>ตอนที่ 1</u> โปรดเลือกตัวเลือกที่ถูกต้องที่สุดเพียงตัวเลือกเดียว (ข้อละ 1 คะแนน)

<u>ตอนที่ 1</u> โปรดเลือกตัวเลือกที่ถูกต้องที่สุดเพียงตัวเลือกเดียว (ข้อละ 1 คะแนน)

1. **ข้อใดถูกไม่ถูกต้องเกี่ยวกับ ISO-27000**

a) มาตรฐาน ISO/IEC 27001 จะเน้นเรื่องข้อกำหนดในการจัดทำระบบ ISMS ให้กับองค์กรตามขั้นตอน Plan-Do-Check-Act และใช้แนวทางในการประเมินความเสี่ยงมาประกอบการพิจารณาเพื่อหาวิธีการหรือมาตรการที่เหมาะสม

b) มาตรฐาน ISO/IEC 17799 จะเน้นเรื่องวิธีปฏิบัติที่จะนำไปสู่ระบบ ISMS ที่องค์กรได้จัดทำขึ้น ซึ่งจะต้องเป็นไปตามมาตรฐาน ISO/IEC 27001 กำหนดไว้ด้วย

c) มาตรฐาน ISO/IEC 27001 มีการกล่างถึงการปฏิบัติตามข้อกำหนด (Compliance)

d) มาตรฐาน ISO/IEC 27001 ครอบคลุมถึงการจัดการเอกสารที่เป็น hard copy ด้วย

e) ไม่มีคำตอบ

2. ใน ISO27000 มี 11 domain ข้อใดไม่ได้กล่าวไว้

a) การควบคุมการเข้าถึง (Access Control)

b) การบริหารการใช้ทรัพยากรเพื่อประโยชน์สูงสุด (Resource Utilization)

c) การจัดหาการพัฒนาและบำรุงรักษาระบบสารสนเทศ (Information systems acquisition, development and maintenance)

d) การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information security incident management)

e) การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business continuity management)

3. หัวข้อใดไม่จำเป็นต้องดำเนินการใน ISO 27000

a) การบริหารจัดการทรัพย์สินขององค์กร (Asset management)

b) ความมั่น คงปลอดภัยที่เกี่ยวข้องกับบุคลากร

5. ข้อใดมีความจำเป็นน้อยที่สุดที่ต้องมีในการทำ Asset Management

a) มีชื่อของอุปกรณ์

b) แสดงชนิดของอุปกรณ์

c) แสดงตำแหน่งติดตั้งอุปกรณ์

d) แสดงชื่อผู้รับผิดชอบอุปกรณ์แต่ละอุปกรณ์

e) แสดงชื่อผู้ใช้งานเป็นรายอุปกรณ์

6. การทำ Information classification ในเรื่อง Asset Management ข้อใดควรทำ "น้อยที่สุด"

a) Label marking(e.g. Confidential)

b) การจัดหมวดหมู่

c) การแยกสถานที่

d) การทำสำรองมากกว่า 1 ชุด

e) การระบุผู้รับผิดชอบ

7.ข้อใดไม่ได้กำหนดไว้ในการควบคุมการเข้าถึง (Access Control)

a) การควบคุมการเข้าถึงเครือข่ายที่ไม่ได้รับอนุญาต

b) การควบคุมการเข้าถึงระบบปฏิบัติการที่ไม่ได้รับอนุญาต

c) การควบคุมการเข้าถึง Application และสารสนเทศที่ไม่ได้รับอนุญาต

d) การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอก

e) ไม่มีข้อถูก

8.ข้อใดเกี่ยวข้องกับ Physical and environment securityมากที่สุด

a) Equipment maintenance

b) Control room access

c) Public access

d) Removal of property

e) ถูกทุกข้อ

9.ข้อใดไม่เกี่ยวข้องกับ Information systems acquisition, development

<u>ตอนที่ 1</u> โปรดเลือกตัวเลือกที่ถูกต้องที่สุดเพียงตัวเลือกเดียว (ข้อละ 1 คะแนน)

(Human resources security) c) การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security) d) การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศ (Communication and operations management) e) ไม่มีข้อถูก	**and maintenance** a) Correct processing in applications b) Security requirements of information systems c) Cryptographic controls d) Personal assessment e) Security in development and support processes
4.ข้อใดเป็น Asset ที่เกี่ยวข้องน้อยที่สุดในการทำ Asset Management a) Electricity b) Database c) software d) IT Staff e) Network link	
10.จากข้อมูลที่ให้ในรูป ท่านคิดว่าเกี่ยวข้องกับหัวข้อใดมากที่สุด	a) นโยบายความมั่นคงปลอดภัยขององค์กร (Security policy) b) ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human resources security) c) การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม(Physical and environmental security) d) การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศ (Communication and operations management) e) การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business continuity management)
	12. ข้อใดไม่จริงในเรื่องความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human resources security) a) กล่าวถึงบทบาทของผู้บริหารสารสนเทศ หัวหน้างานสารสนเทศ หัวหน้างานบุคคลและหัวหน้างานที่เกี่ยวข้องในต่างๆ ดังต่อไปนี้

<u>ตอนที่ 1</u> โปรดเลือกตัวเลือกที่ถูกต้องที่สุดเพียงตัวเลือกเดียว (ข้อละ 1 คะแนน)

a) Access Management b) Capacity Management c) Network Management d) Database Management e) Risk Management **11.ข้อใดใน 11 domain ของ ISO27000 เกี่ยวข้องกับรูปข้างล่างนี้มากที่สุด**	b) โครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กร เพื่อบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร c) การ สร้างความมั่นคงปลอดภัยก่อนการจ้างงาน เพื่อให้พนักงานและผู้เกี่ยวข้องจากหน่วยงานภายนอกเข้าใจถึงบทบาทและหน้าที่ความรับผิดชอบของตน และเพื่อลดความเสี่ยงอันเกิดจากการขโมย การฉ้อโกง และการใช้อุปกรณ์ผิดวัตถุประสงค์ d) การสร้างความ มั่นคงปลอดภัยในระหว่างการจ้างงาน เพื่อให้พนักงานและผู้เกี่ยวข้องจากหน่วยงานภายนอกได้ตระหนักถึงภัยคุกคาม และปัญหาที่เกี่ยวข้องกับความมั่นคงปลอดภัย หน้าที่ความรับผิดชอบและทำความเข้าใจกับนโยบาย เพื่อลดความเสี่ยงอันเกิดจากความผิดพลาดในการปฏิบัติหน้าที่ e) การ สิ้นสุดและการเปลี่ยนการจ้างงาน เพื่อให้พนักงานและผู้เกี่ยวข้องจากหน่วยงานภายนอกได้ทราบถึงหน้าที่ความ รับผิดชอบและบทบาทของตน เมื่อสิ้นสุดการจ้างงานหรือมีการเปลี่ยนการจ้างงาน
13. **จากผลลัพธ์ที่แสดง ขั้นตอนใดที่น่าจะเกี่ยวข้องมากที่สุด**	

<u>ตอนที่ 1</u> โปรดเลือกตัวเลือกที่ถูกต้องที่สุดเพียงตัวเลือกเดียว (ข้อละ 1 คะแนน)

a) Risk assessment
b) Asset control
c) Review of the information security control
d) Authorization process for information processing facilities
e) Confidentiality agreements

<u>ให้ตอบว่าข้อความที่ให้ไว้ ถูก (T) หรือ ผิด (F)</u>

14. การจัดหา การพัฒนาและการบำรุงรักษาระบบสารสนเทศ (Information systems acquisition, development and maintenance) มีการกำหนดให้มีการสร้าง ความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์ เพื่อสร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์และในการ ใช้งาน

a) T b) F

<u>ข้อความต่อไปนี้ ใช้สำหรับตอบคำถามข้อ 16-25 ข้างล่างนี้</u>

นาย ก. เป็นพนักงานแผนกเทคโนโลยีสารสนเทศ มีหน้าที่ในการดูแลระบบสารสนเทศของบริษัทฯให้สามารถทำงานได้ตามปกติ
แล้ววันหนึ่งระบบเครือข่ายของบริษัทฯ ล่ม ทำให้สูญเสียรายได้ของบริษัทฯมาก

16.นาย ก. ควรปฏิบัติอย่างไร

a) กู้ระบบขึ้นมาทันที
b. แก้ไขปัญหาสาเหตุของการล่มของระบบ
c. ติดต่อ Product's Specialist
d. ปฏิบัติ Incident Response Plan
e. ไม่มีข้อใดถูกต้อง

17.การที่ระบบล่มนั้น ส่งผลต่อบริษัทฯเป็นอย่างมาก เป็นเพราะว่า นาย ก. ไม่ได้เตรียมเรื่องใด

a. AIA
b. BIA
c. CIA

<u>ตอนที่ 1</u> โปรดเลือกตัวเลือกที่ถูกต้องที่สุดเพียงตัวเลือกเดียว (ข้อละ 1 คะแนน)

15.ในหัวข้อโครงสร้างด้านความมั่นคงปลอดภัยสำหรับองค์กร (Internal organization) โดยได้กล่าวถึงบทบาทของผู้บริหารองค์กรและหัวหน้างานสารสนเทศ
ในหัวข้อที่เกี่ยวกับโครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กร
เพื่อบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

a) T b) F

19.ก่อนหน้าที่ระบบจะล่มลง นาย ก. ควรจะหาข้อมูลถึงผลกระทบต่างๆที่มีต่อบริษัทฯ โดย

a. ค้นหาข้อมูลจากการ survery
b. ค้นหาข้อมูลจากการสัมภาษณ์
c. คัดเลือกผู้ถูกสัมภาษณ์
d. ถูกทุกข้อ
e. ไม่มีข้อใดถูกต้อง

20.ข้อมูลผลกระทบต่างๆ ที่มีต่อบริษัทฯ จากข้อข้างต้นนั้น ควรเป็นแบบใด

a) ข้อมูลที่เกี่ยวข้องกับการเงิน
b. ข้อมูลที่เกี่ยวข้องกับลูกค้า
c. ข้อมูลที่เกี่ยวข้องกับธุรกิจที่สำคัญ
d. ถูกทุกข้อ
e. ไม่มีข้อใดถูกต้อง

21.นาย ก. ต้องพิจารณาถึง

d. DIA
e. ไม่มีข้อใดถูกต้อง

18.เวลาที่บริษัทฯสามารถรอได้นานที่สุดจนกระทั่งระบบกลับมาทำงานใหม่ เรียกว่า

a. MTD
b. TTD
c. DTM
d. DDT
e. ไม่มีข้อใดถูกต้อง

24.นาย ก. วางแผนแล้ว ควรจะดำเนินการอะไรต่อไป

a. ดำเนินการสร้างระบบเทคโนโลยีสารสนเทศให้รองรับ
b. ทดสอบแผนที่วางไว้ เป็นระยะๆ
c. ติดต่อผู้ที่เกี่ยวข้องในแผนให้รับทราบ
d. ถูกทุกข้อ
e. ไม่มีข้อใดถูกต้อง

25.บริษัทฯ ได้ทราบถึงความเสียหายที่เกิดขึ้นกับระบบที่ นาย ก. ดูแล บริษัทฯ ควรทำอย่างไร

a. ไล่ นาย ก. ออกจากงาน
b. ทำทัณฑ์บน นาย ก.
c. ไม่ทำอะไร นาย ก. เพราะนาย ก. ทำดีที่สุดแล้ว
d. สร้างระบบใหม่

<u>ตอนที่ 1</u> โปรดเลือกตัวเลือกที่ถูกต้องที่สุดเพียงตัวเลือกเดียว (ข้อละ 1 คะแนน)

ระยะเวลาในการนำการให้บริการ การดำเนินการ กิจกรรม และสิ่งที่เกี่ยวข้อง คืนมาหลังจากเกิดเหตุการณ์ฉุกเฉิน หมายถึง นาย ก. ต้องคำนึงถึงข้อใด

a. System Recovery Time

b. Recovery Time Objective

c. System Startup Time

d. System Ready Time

e. ไม่มีข้อใดถูกต้อง

22.นาย ก. ควรจะมีการวางแผนอะไร เพื่อแก้ปัญหาระบบเทคโนโลยีสารสนเทศล่มได้ดีที่สุด

a. BCP

b. DCP

c. BRP

d. DRP

e. ไม่มีข้อใดถูกต้อง

23.นาย ก. ควรดำเนินการวางแผนที่รองรับการแก้ปัญหาธุรกิจของบริษัทฯ ที่มีผลกระทบจากปัญหาข้างต้น

a. BCP

b. DCP

c. BRP

d. DRP

e. ไม่มีข้อใดถูกต้อง

e. ไม่มีข้อใดถูกต้อง

26. ข้อใดไม่ใช่ส่วนประกอบของ Security & Risk Management

a) Policy b) Asset c) Remediate

d) Protection e) Access Point

27. ข้อใดไม่ใช่ส่วนประกอบของ Protection Technology

a) IPS b) Firewall c) Anti Virus

d) Switching e)Lock Screen

28. การทำ Security & Risk Management จำเป็นต้องมีกระบวนการใดเป็นสิ่งแรก

a) Policy b) Compliant

c) Asset Prioritize

d) Vulnerability Assessment

e) Protection

29. สิ่งใดเกี่ยวข้องกับองค์ประกอบของ Risk Measurement

a) Asset b) Vulnerability

c) Threat

d) ถูกทุกข้อ e) ไม่มีข้อใดถูกต้อง

30. อุปกรณ์ IT ใดไม่เกี่ยวข้องกับ IT Security & Risk Management

a) Mouse b) Keyboard

c) LCD Monitor

d) ข้อ a และ b e) ข้อ a และ c

31. การทำ Security & Risk Management เกี่ยวข้องกับกระบวนการใด

a) People b) Process

c) Technology

d) ถูกทุกข้อ e) ไม่มีข้อใดถูกต้อง

<u>ตอนที่ 1</u> โปรดเลือกตัวเลือกที่ถูกต้องที่สุดเพียงตัวเลือกเดียว (ข้อละ 1 คะแนน)

32. ข้อใดไม่ใช่มาตรฐานการทำ Security Policy แบบสากล

a) SOX b) ITIL c) PCIDSS d) ISO27000 e) HIPAA

33. ผลที่ได้จากการทำ Security & Risk Management คืออะไร

a) ทำงานมีประสิทธิภาพมากขึ้น

b) การป้องกันภัยคุกคามได้ดีขึ้น

c) มีมาตรฐานในการทำงานที่ปลอดภัย

d) ระบบมีความเสถียรมากขึ้น

e) ถูกทุกข้อ

34.SOC ย่อมาจากอะไร

a) Security Opportunity Center

b) Security Officer Center

c) Security Operation Center d) Security Occupation Center

e) Security Operation Counter

35. เหตุใดจึงต้องมีการทำ SOC

a) ระบบไม่มีมาตรฐานการทำงานที่ปลอดภัยเพียงพอ

b) เครื่อง Endpoint สามารถลงโปรแกรมอะไรก็ได้

c) เครื่อง Endpoint สามารถเสียบ USB Modem ได้

d) ปัญหา Security Issues ไม่สามารถเชื่อมโยงปัญหาที่เกิดขึ้นได้ e) ถูกทุกข้อ

36. หากบ้านพักอาศัยของเรา

39.เราจะเพิ่มค่าของตัวเรา ในเรื่องที่เกี่ยวข้องกับ Security & Risk Management ได้อย่างไร

a) ควรเข้างานและเลิกงาน ตรงเวลาที่กำหนด

b) ควรแบ่งปันเครื่องคอมพิวเตอร์ให้เพื่อนร่วมงานใช้

c) ควรให้เพื่อนยืม USB Thumb Drive

d) โหลดหนังจาก BIT ให้เพื่อนๆดูกัน

e) ไม่มีข้อใดถูกต้อง

40. ข้อใดที่ทำให้การบังคับใช้ Security & Risk Management ไม่ได้ผล

a) อนุญาตให้ติดตั้ง program อะไรก็ได้บนเครื่อง Endpoint

b) ให้เพื่อนเล่นเกมออนไลน์บนเครื่องคอมฯของบริษัทฯ

c) อนุญาตให้นำเครื่องส่วนตัวมาต่อกับเนทเวอร์คของที่ทำงานได้

d)อนุญาตให้เข้าปลูกผักในเฟสบุคได้

e) ถูกทุกข้อ

41) อุปกรณ์ IT ข้อใดเปรียบเสมือนกล้องวงจรปิด

a) IDS b) IPS c) Firewall d) Switching Hub e) ถูกทุกข้อ

42) อุปกรณ์ IT ข้อใดเปรียบเสมือนกุญแจประตูบ้าน

a) IDS b) IPS c) Firewall d) Switching Hub e) ถูกทุกข้อ

43) Proxy มีไว้เพื่ออะไร

a) เพื่อให้มีการตรวจสอบได้ง่ายขึ้น b) เพื่อให้ทำงานได้เร็วขึ้น

c) เพื่อให้เกิดความซับซ้อนในระบบมากขึ้น d) ข้อ a และ b

e) ถูกทุกข้อ

<u>ตอนที่ 1</u> โปรดเลือกตัวเลือกที่ถูกต้องที่สุดเพียงตัวเลือกเดียว (ข้อละ 1 คะแนน)

มีแค้มป์คนงานก่อสร้างต่างชาติมาตั้งอยู่ จะเป็นการเพิ่มให้ค่าให้ข้อใด

a) Vulnerability b) Remediation c) Protection d) Prioritize e) Policy

37. การที่มีข่าวเผยแพร่การเจาะตู้เซฟของร้านทอง โดยการดัดแปลงอุปกรณ์ที่ใช้เพื่อตัดลูกกรงเหล็ก เป็นการเพิ่มค่าอะไรในการระบวนการ Security & Risk Management

a) Vulnerability b) Threat c) Asset d) ถูกทุกข้อ e) ไม่มีข้อใดถูกต้อง

38. การที่รายการตีสิบนำวิธีการโจรกรรมรถยนต์มาเผยแพร่เป็นการเพิ่มค่าอะไรในกระบวนการวัดค่า Risk

a) Policy b) Risk Level c) Threat Level d) Vulnerability Level e) ข้อ b, c, d

44) จากข่าวการถูกหลอกให้โอนเงินผ่านตู้เอทีเอ็มทั้งๆที่มี SMS ระบุรหัส One Time Password และระบุเบอร์บัญชีโดยหลักการแล้วคุณคิดว่าเป็นความรับผิดชอบของใคร

a) ธนาคารเจ้าของตู้เอทีเอ็ม b) ผู้โอนเงิน c) ผู้ที่ได้รับโอนเงิน d) ไม่มีผู้ใดต้องรับผิดชอบ e) ทุกฝ่ายต้องรับผิดชอบ

45) เทคโนโลยีใดไม่เกี่ยวกับ Physical Security

a) Host NAC b) Port Control for Endpoint c) Fingerprint Scanning d) Routing Management e) ถูกทุกข้อ

46. การกระทำข้อใดไม่เกี่ยวข้องกับ Physical Security

a) การที่ตู้ ATM มีสายต่อ Router, Modem โผล่ออกมานอกตู้
b) การที่เซ็นทรัลล๊อกของรถยนต์เสียแล้วไม่ซ่อม
c) ประตูอัตโนมัติของรถเมล์เสีย ไม่สามารถปิดได้
d) การเซ็ท Firewall ผิด ทำให้ส่งข้อมูลไปผิดที่
e) ถูกทุกข้อ

47. ใครเป็นผู้รับผิดชอบต่อข้อมูลขององค์กร

a) ทีม IT b) ผู้ใช้งาน c) ผู้ปรับปรุงข้อมูล d) หน่วยงานที่ใช้ข้อมูล e) ถูกทุกข้อ

48.

52. ถ้า นาย ก. เข้าไปตรวสอบแล้วพบว่าโดนไวรัสโจมตีระบบอยู่ นาย ก. ควรดำเนินการดังนี้

a. ปิดระบบทันที เพื่อไม่ให้ไวรัสลุกลาม
b. ไม่ทำอะไร เพราะ ทำอะไรไม่ได้
c. Update pattern virus ใหม่ให้กับระบบ Antivirus
d. ถูกเฉพาะข้อ a และ c
e. ไม่มีข้อใดถูกต้อง

53. ถ้านาย ก. เข้าไปตรวสอบแล้วพบว่ามีผู้ไม่ประสงค์ดีกำลังเจาะระบบฐานข้อมูลอยู่ นาย ก. ควรดำเนินการดังนี้

<u>ตอนที่ 1</u> โปรดเลือกตัวเลือกที่ถูกต้องที่สุดเพียงตัวเลือกเดียว (ข้อละ 1 คะแนน)

เราควรใช้เทคโนโลยีใดในการทำให้เครื่องคอมพิวเตอร์มีเวลาที่ตรงกับระบบขององค์กร
a) OTP b) NTP c) NAC d) HIPS e) ถูกทุกข้อ

49.
เราจะป้องกันข้อมูลในเครื่องคอมฯรั่วไหลด้วยเทคโนโลยีอะไร
a) NAC b) AntiVirus c) Disk Encryption
d) File & Folder Encryption e) Data Loss Prevention

50. สิ่งใดที่จัดอยู่ใน Concept & Protection in Physical Environment
a) ต้องมี password ในการเข้าสู่การใช้งาน Windows OS
b) ต้องมี password สำหรับ lock หน้าจอเครื่องขณะไม่ได้ใช้งาน c) ต้องมี Disk Encryption เพื่อรักษาความปลอดภัยข้อมูล
d) ต้องไม่พูดเรื่องเกี่ยวกับงานในลิฟท์ที่มีคนแปลกหน้าอยู่
e) ถูกทุกข้อ

<u>ข้อความต่อไปนี้ ใช้สำหรับตอบคำถามข้อ 51- 55</u>

นาย ก. เป็นพนักงานแผนกเทคโนโลยีสารสนเทศ มีหน้าที่ในการดูแลระบบสารสนเทศของบริษัทฯให้สามารถทำงานได้ตามปกติ
แล้ววันหนึ่งได้รับแจ้งจากผู้ใช้ว่าระบบเครือข่ายของบริษัทฯ ทำงานช้าลงอย่างเห็นได้ชัด

51. นาย ก.
ได้ดำเนินการติดต่อไปที่พนักงานท่านนั้นทันที นาย ก. ทำถูกต้องหรือไม่

a. ถูกต้อง เพราะ นาย ก. ต้องตรวจสอบข้อมูลเบื้องต้นก่อน
b. ถูกต้อง เพราะ นาย ก. ต้องหาผู้ผิด
c. ไม่ถูกต้อง เพราะ นาย ก. ควรทำตามกระบวนการที่กำหนดไว้
d. ไม่ถูกต้อง เพราะ ปิดระบบทันที เพื่อไม่ให้ผู้ไม่ประสงค์ดีได้ข้อมูลไป
b. ไม่ทำอะไร เพราะ ทำอะไรไม่ได้
c. เปลี่ยนสิทธิการเข้าระบบฐานข้อมูลใหม่ทั้งหมด
d. ถูกเฉพาะข้อ a และ c
e. ไม่มีข้อใดถูกต้อง

54. นาย ก. ทำอย่างไร ปัญหาจะถูกแก้ไขได้อย่างถูกวิธี

a. วางแผนการรับมือกับเหตุการณ์ในกรณีต่างๆ
b. อบรมบุคลากรให้รู้วิธีการรับมือ
c. ปฏิบัติตามแผนการรับมือ
d. ถูกทุกข้อ
e. ไม่มีข้อใดถูกต้อง

55. ถ้านาย ก. ต้องการปรับปรุงการทำงานของตน ควรทำอย่างไรดีที่สุด

a. ตั้งระบบตรวจสอบทุกจุด เพื่อเตือนผู้ดูแลระบบเมื่อเกิดเหตุการณ์ผิดปกติ
b) ทดสอบระบบก่อนทำงานจริง
c. แจ้งผู้ใช้ให้ทราบถึงปัญหาที่เกิดขึ้นก่อนเข้าไปปฏิบัติการ แก้ไข
d) ถูกทุกข้อ
e) ไม่มีข้อใดถูกต้อง

56. Electronic vaulting มีส่วนประกอบอะไรบ้าง

a. Online tape vaulting
b. Remote journaling
c. Database shadowing

<u>ตอนที่ 1</u> โปรดเลือกตัวเลือกที่ถูกต้องที่สุดเพียงตัวเลือกเดียว (ข้อละ 1 คะแนน)

พนักงานคนนั้นไม่ได้เป็นผู้กระทำผิด

e. ไม่มีข้อใดถูกต้อง

57. Identify the response procedures, including:

a. Evacuation and safety of personnel

b. Notification of disaster

c. Initial damage assessment

d. ถูกทุกข้อ

e. ไม่มีข้อใดถูกต้อง

58. ข้อเสียของ cold site คือ

a. Operational testing is not possible

b. Organizations have exclusive use

c. Practical for less-popular hardware configurations

d. ไม่มีข้อใดถูกต้อง

e. ถูกทุกข้อ

59. ข้อดีของ warm site คือ

a. Operational testing is not possible

b. Practical for less-popular hardware

d. ถูกทุกข้อ

e. ไม่มีข้อใดถูกต้อง

c) Object-Oriented Database Management Systems

d) ถูกเฉพาะข้อ a และ c

e) ถูกทุกข้อ

63. An attribute or set of attributes that uniquely identifies a specific instance of an entity is

a) Primary key b) Private key c) Single key

d) ไม่มีข้อใดถูกต้อง e) ถูกทุกข้อ

64. The main components of a database using SQL include:

a) Windows b) Views c) Linux

d. ไม่มีข้อใดถูกต้อง e) ถูกทุกข้อ

65) The threats to a DBMS include:

a. Aggregation b) Bypass attacks c)Concurrency

d) ไม่มีข้อใดถูกต้อง e) ถูกทุกข้อ

66. ภาษาที่ใช้ในการเขียน program ในปัจจุบันมีกี่ generations

<u>ตอนที่ 1</u> **โปรดเลือกตัวเลือกที่ถูกต้องที่สุดเพียงตัวเลือกเดียว (ข้อละ 1 คะแนน)**

configurations

c. More expensive than cold site or in-house recovery sites.

d. ไม่มีข้อใดถูกต้อง

e. ถูกทุกข้อ

60. การอบรมแผนต่อเนื่องทางธุรกิจ ควรจะประกอบด้วย

a. Describe the recovery organization (teams and functions).

b. Explain the flow of recovery events and activities following a disaster

c. State team members' responsibilities in recovery activities

d) ไม่มีข้อใดถูกต้อง

e) ถูกทุกข้อ

61. อะไรเป็นภัยสำหรับ software

a. Buffer Overflow

b. b) Malware

c. Social Engineering

d. d) ถูกเฉพาะข้อ a และ b

e. ถูกทุกข้อ

62. The various architecture models that exist for databases are:

a. Hierarchical Database Management Systems

b. Spreadsheets

a) 1 b) 2 c) 3 d) 4 e) 5

67. ข้อใดเป็นภาษาที่ใช้ในการเขียน program

a) Machine language b) Natural language

c) High level language d) ถูกทุกข้อ

e) ไม่มีข้อใดถูกต้อง

68. The original Java security model implemented

a) firewall b) antivirus c) sandbox

d) coding e) ไม่มีข้อใดถูกต้อง

69.ข้อใดถูกต้องสำหรับ Java Secure Socket Extension (JSSE)

a)ใช้ Secure Socket Layer protocol
b) ใช้ Transport Layer Security protocol

c).ใช้ IPSec Protocol
d) ถูกเฉพาะข้อ a และ b
e) ถูกทุกข้อ

70. OLTP systems should act as a monitoring system and provide the following:

a) Detect when individual processes abort

b. Automatically restart an aborted process

c) Back out of a transaction if necessary

d) ถูกทุกข้อ

<u>ตอนที่ 1</u> โปรดเลือกตัวเลือกที่ถูกต้องที่สุดเพียงตัวเลือกเดียว (ข้อละ 1 คะแนน)

71.ในมุมมองของ Security ลายเซ็นบุคคลถือเป็นการพิสูจน์ตัวตน (Authentication) ในข้อใดดังต่อไปนี้

a. Something you know

b. Something you have

c. Something you are

d. Something you know และ Something you have

e. Something you are, Something you know และ Something you have

72. ในมุมมองของ Security วิธีการส่ง OTP (One time password) ผ่านทาง SMS มือถือเป็นการพิสูจน์ตัวตน (Authentication) ในข้อใดดังต่อไปนี้

a. Something you know

b. Something you have

c. Something you are

d. Something you know และ Something you have

e. Something you are, Something you know และ Something you have

73.วิธีการควบคุมการจัดการความปลอดภัย (Control of security management) เกี่ยวข้องกับ ข้อใดน้อยที่สุด

a. จัดให้มียามเดินตรวจตราและดูแลรักษาความปลอดภัยในทุกส่วนของสถานที่

b. จัดให้มีการฝึกอบรมให้กับแม่

e. ไม่มีข้อใดถูกต้อง

75.ข้อใดต่อไปนี้เป็นวิธีการโจมตีโดยอาศัยหลักการแบบ Man in the middle Attack

a) Teardrop attack

b) DDoS (Distributed Denial of Service) attack

c) Arp spoofing attack

d) Smurf attack

e) RFI (Remote file inclusion) attack

76.วิธีการในข้อใดต่อไปนี้สามารถใช้พิสูจน์ความคงสภาพของข้อมูล (Integrity) และป้องกันการปฏิเสธความรับผิดชอบในการทำ (non-repudiation) ได้ดีที่สุด

a. การเก็บFileข้อมูล ลงบนเครื่องคอมพิวเตอร์ที่ Hard disk ทำRaid 5 ไว้

b. การทำ Message digest ของFile ข้อมูลด้วย Algorithm MD5 และส่งFileข้อมูลกับ MD5 Checksum ให้กับผู้รับ

c. การรับ-ส่งข้อความทาง E-Mail โดยใช้ PKI (Public Key Infrastructure)

d. การเข้ารหัส File ข้อมูล ด้วย Algorithm 3DES

<u>ตอนที่ 1</u> โปรดเลือกตัวเลือกที่ถูกต้องที่สุดเพียงตัวเลือกเดียว (ข้อละ 1 คะแนน)

บ้าน ทุกๆเดือน

c. ติดตั้งFirewall ในทุก Network Segment

d. ตรวจสอบประวัติของผู้มาติดต่อ

e. ปรับปรุงสวัสดิการและเงินเดือนของพนักงาน

74.ข้อใดถือเป็นหลักการสำคัญมากที่สุดในการเข้ารหัสข้อมูล (cryptography)

a. ทำให้ผู้ไม่หวังดี ไม่สามารถถอดรหัสข้อมูลที่เข้ารหัสแล้ว ได้

b. ทำให้ผู้ไม่หวังดี ต้องใช้เวลาถอดข้อมูลที่เข้ารหัสแล้วยาวนานมากว่าระยะเวลาที่ต้องการคงความลับของข้อมูลนั้นไว้

c. ทำให้ผู้ไม่หวังดี ล้มเลิกความพยายามที่จะถอดรหัสข้อมูลที่เข้ารหัสแล้ว

d. ทำให้ผู้ไม่หวังดี ต้องจ้างผู้เชี่ยวชาญในการถอดรหัสมาถอด

e. ทำให้ข้อมูลที่นำมาเข้ารหัสเป็นความลับตลอดไป

79. ข้อใดต่อไปนี้เป็นข้อมูลที่ถูกต้อง

e. ไม่มีข้อถูก

77.PKI (Public Key Infrastructure) สามารถสนองความต้องการด้านความปลอดภัยได้ยกเว้นข้อใดต่อไปนี้

a) ความลับ (Confidentiality)

b) ความคงสภาพ (Integrity)

c) ความพร้อมใช้งาน (Availability)

d) การปฏิเสธความรับผิดชอบในการทำ (non-repudiation)

e) การระบุตัวตน (Identification)

78.การกระทำในข้อใดต่อไปนี้เป็นรูปแบบการโจมตีแบบ Social Engineering ที่ชัดเจนที่สุด

a) ส่งSpam E-mail ให้เป้าหมาย

b) การหลอกถามข้อมูลส่วนตัวต่างๆของเป้าหมาย

c) การแอบลักลอบดักฟังโทรศัพท์ของเป้าหมาย

d) การแอบดูรหัสผ่านระหว่างเป้าหมายกำลังพิมพ์รหัสผ่าน

e) ถูกทุกข้อ

83. _____is a processing or

<u>ตอนที่ 1</u> โปรดเลือกตัวเลือกที่ถูกต้องที่สุดเพียงตัวเลือกเดียว (ข้อละ 1 คะแนน)

a. WPA สามารถรองรับการเข้ารหัสแบบTKIP เท่านั้น แต่ WPA2 สามารถรองรับการเข้ารหัสแบบTKIP และแบบ CCMP

b. WPA และ WPA2 ไม่สามารถรองรับการเข้ารหัสแบบ CCMP ได้

c. WEP และ WPA-TKIP ใช้ Encryption Algorithm คนละแบบ

d. โทรศัพท์มือถือแบบ GSM ใช้เทคโนโลยีการแบ่งช่องสัญญาณ แบบ FDMA (Frequency Division Multiple Access)

e. ไม่มีข้อถูก

80.ข้อใดต่อไปนี้เป็นข้อมูลที่ไม่ถูกต้อง

a) อุปกรณ์ Firewall จัดเป็น อุปกรณ์ Access Control ชนิดหนึ่ง
b) การพิสูจน์ตัวตน (Authentication) โดยใช้ RFID Card จัดเป็น something you have

c. การเข้ารหัสแบบ 3DES ถือเป็นการเข้าแบบ Symmetric Encryption

d. MD5 Checksum จัดเป็น ECC string (Error Checking and Correcting string)

e. ไม่มีข้อถูก

81._____is an action that compromises the security of information owned by an organization.

a. Security attack

b. Security service

communication service that enhances the security of the data processing systems and the information transfers of an organization.

a. Security attack

b. Security goal

c. Security service

d. Security mechanism

e. None of the above

84. _____is an attack that attempts to learn or make use of information from the system but does not affect system resources.

a. Passive attack

b. Denial of service

c. A masquerade

d. A replay

e. None of the above

85._____takes place when one entity pretends to be a different entity.

a. A masquerade

b. A replay

c. Traffic analysis

d. A masquerade

e. None of the above

86._____involves the passive capture of data unit and its subsequent

<u>ตอนที่ 1</u> **โปรดเลือกตัวเลือกที่ถูกต้องที่สุดเพียงตัวเลือกเดียว (ข้อละ 1 คะแนน)**

c. Security mechanism

d. Security system

e) None of the above

82._____is a process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.

a) Security service

b) Security attack

c) Security provider

d) Security mechanism

e) None of the above

88. Which of the following is not related to <u>authentication service</u>?

a. Concerns with assuring that a communication is authentic.

b. To assure the recipient that the received message is from the source that it claims to be from.

c. Assures that the two entities are the the entities that they claim to be.

d. The ability to limit and control the access to host

retransmission to produce an unauthorized effect.

a. A disruption of the entire network

b. An overloading the network with messages

c. A replay

d. Traffic analysis

e. None of the above

87._____prevents the normal use or management of communication facilities.

a. A masquerade

b. Denial of service

c. A replay

d) An eavesdropping

e) None of the above

92._____is software that is intentionally inserted in a system for a harmful purpose.

a. Malicious software

b. Worm

c. Virus

d. Bacteria

<u>ตอนที่ 1</u> **โปรดเลือกตัวเลือกที่ถูกต้องที่สุดเพียงตัวเลือกเดียว (ข้อละ 1 คะแนน)**

systems and applications.

e. None of the above

89. Which of the following choice is not related to encryption

a. Scramble messages.

b. The addition of a code based on the contents of the message.

c. Some secret information shared by the two principles.

d. Procedures used to provide particular services.

e. None of the above

90._____is a process of attempting to discover the plaintext.

a. Cryptanalysis

b. Ciphertext

c. Stream cipher

d. Cryptography

e. None of the above

91._____is designed to divert an attacker from accessing critical systems.

a. IDS

b. IPS

c. <u>Honeypot</u>

d) Firewall

e. None of the above

93._____is a program that can replicate itself and send copies from computer to computer across networks.

a) Malicious software

b) Worm

c) Virus

d) Bacteria

e) None of the above

94.Each of the following factors illustrates why information security is increasingly difficult *except*_____.

a) faster computer processors

b) growing sophistication of attacks

c) faster detection of weaknesses

d) distributed attacks

e) None of the above

95.The primary goal of information security is to protect _____ .

a. procedures

b. people

c. information

d. products

e. None of the above

e) None of the above

97.One reason employees are so successful at attacking their company's computers is _____ .

a. they have superior networking skills

b. employees already have access to all company information

c. a company information security is focused on keeping out intruders

d. employees have unlimited access to company computers

e. None of the above

98.Each of the following is a goal of cyberterrorists *except* _____ .

a. defacing electronic information

b. denying service to legitimate user

c. committing unauthorized intrusion into critical infrastructures

d. replacing computers with unauthorized devices

96.Each of the following is a characteristic of information *except*

a. integrity

b. confidentiality

c. conformity

d. availability

e. None of the above

d. Wireless Application protoco

e) None of the above

102._____ attempts to hide the existence of data.

a) Cryptography

b) Decryption

c) Steganography

d) Hidden Data Resource (HDR)

e) None of the above

103.The _____ was specifically

<u>ตอนที่ 1</u> **โปรดเลือกตัวเลือกที่ถูกต้องที่สุดเพียงตัวเลือกเดียว (ข้อละ 1 คะแนน)**

e. None of the above

99. Each of the following is a reason that software is susceptible to attacks *except* _____ .

a. cost

b. length and complexity

c. extensibility

d. connectivity

e. None of the above

100.Each of the following attacks can be launched using e-mail *except* _____ .

a. man-in-the-middle

b. virus

c. worm

d. Trojan horse

e. None of the above

101.IP Security (IPSec) confidentiality is performed by the _____ protocol.

a. Encapsulating Security Playload protocol

b. Internet Security Association and Key Management Protocol

c. Authentication Header protocol

designed to replace the weaker Data Encryption Standard (DES).

a. IPSec

b. 3DES

c. RSA

d. MD

e. None of the above

104.The _____ defines the overall process involved with developing a security policy.

a. security policy cycle

b. risk identification cycle

c. monitoring scope

d. evaluation cycle

e. None of the above

105. A(n) _____ outlines the actions to be performed when a security breach occurs.

a. security policy

b. incidence response policy

c. security policy cycle

d. risk identification cycle

e. None of the above

106.Each of the following is a category of security protection that can be implemented using WLAN s *except*

<u>ตอนที่ 1</u> โปรดเลือกตัวเลือกที่ถูกต้องที่สุดเพียงตัวเลือกเดียว (ข้อละ 1 คะแนน)

107.MAC address filtering can be implemented by either permitting or _____ a device.

a. preventing

b. configuring

c. throttling

d. encrypting

e. None of the above

108._____ involves sending an e-mail or displaying a Web announcement that falsely claims to be from a legitimate enterprise in an attempt to trick the user into surrendering information.

a) Phishing

b) Social Engineering

c) Resource allocation

d) Web posting

e) None of the above

109.Wireless location mapping refers to passive wireless discovery, also known as

a) wardriving

b) wireless address allocation (WAA)

c) spear driving

d) access point collecting

a) access control

b) wired equivalent privacy (WEP)

c) access restriction

d) authentication

e) None of the above

a. virus

b. worm

c. adware

d. Trojan

e. None of the above

113.Each of the following may indicate a virus has infected a wireless laptop *except*

a. A program suddenly disappears from the computer

b. New programs do not install properly

c. The Service Set Identifier (SSID) changes from uppercase to lowercase

d. Out-of-memory error messages appear

ตอนที่ 1 โปรดเลือกตัวเลือกที่ถูกต้องที่สุดเพียงตัวเลือกเดียว (ข้อละ 1 คะแนน)

e) None of the above

110. Authentication is based on each of the following *except*

a) What you have

b) What you purchase

c) What you know

d) What you are

e) None of the above

111.Each of the following is a characteristic of a weak password *except*

a. Using a common word

b. Changing a password every 30 days

c. Short passwords

d. Using the same passwords for all accounts

e. None of the above

112. A(n) _____ must attach itself to a computer document, such as an e-mail message, and is spread by traveling along with the document.

118.จากรูปด้านล่างเป็นการทดสอบความปลอดภัยของเว็บไซต์แห่งหนึ่ง

e. None of the above

114.การทดสอบความมั่นคงปลอดภัยโดยการเจาะระบบ (Penetration Testing) แบบใดที่มีความใกล้เคียงกับพฤติกรรมหรือสภาพแวดล้อมของแฮกเกอร์ (Hacker) มากที่สุด

a). Sand box b) Black box
c) Gray box
d). White box e) External box

115.
ข้อใดต่อไปนี้เป็นสิ่งที่ควรทำเป็นอันดับแรกในกระบวนการ Penetration Testing

a) OS fingerprinting b) Port Scanning c) Social Engineering
d) Passive information Gathering e) IP Address Spoofing

116.ข้อใดเป็นประโยชน์ของคำสั่ง telnet ในกระบวนการทำ Penetration Testing

a) ใช้ทดสอบว่าเซิร์ฟเวอร์เปิดให้บริการ DNS บน UDP พอร์ต 53 หรือไม่b) ใช้ตรวจสอบชื่อซอฟต์แวร์และเวอร์ชันของบริการ SSH บนเซิร์ฟเวอร์
c) ใช้ตรวจจับข้อมูลแทนการใช้โปรแกรม Sniffer
d) ใช้ทดสอบ DNS Zone Transfer
e) ใช้ทดสอบความสามารถในการทดต่อการถูกบุกรุกโดย DDoS Attack

117.เครื่องมือใดที่เหมาะสมในการใช้ตรวจสอบรหัสรุ่น (version) ของระบบปฏิบัติการบนคอมพิวเตอร์จากระยะไกลได้

a) dsniff b) nmap c) tcpdump
d) os-probe e) osfinger

<u>ตอนที่ 1</u> โปรดเลือกตัวเลือกที่ถูกต้องที่สุดเพียงตัวเลือกเดียว (ข้อละ 1 คะแนน)

จากผลลัพธ์ที่ได้ดังรูป
สามารถนำผลนี้ไปใช้ในการทดสอบสิ่งใดได้
a) ใช้ข้อมูลนี้ในการเข้าระบบโดยไม่ต้องล็อกอิน (By-passing Authentication)
b) ใช้ทดสอบฐานข้อมูลโดยทำ SQL injection
c) ใช้ทดสอบหาช่องโหว่ของ PHP
d) ใช้ทดสอบหาช่องโหว่ของ IIS
e)
ใช้ทดสอบสภาวะการทนทานต่อการถูกบุกรุกด้วย Dos Attack

119.ข้อใดเป็นการแก้ไขปัญหาของการ Buffer Overflow ในเว็บไซต์ได้ถูกต้องมากที่สุด
a) เปลี่ยนโปรแกรมเว็บเซิร์ฟเวอร์จาก IIS เป็น Apache
b) อัพเดทโปรแกรมเว็บเซิร์ฟเวอร์
c)
ตรวจสอบขนาดหรือความยาวของข้อมูลที่นำเข้าจากหน้าเว็บสร้างไฟล์ .htaccess
เพื่อตรวจสอบผู้ใช้งาน
d) สร้าง Virtual Host

120.ข้อแตกต่างที่ชัดเจนในการทำ Penetration Testing โดยใช้การทดสอบแบบ Automated Testing และ Manual Testing คืออะไร
a) Manual Testing
จะใช้เวลาในการทดสอบเร็วกว่า Automated Testing
b) Automated Testing
จะให้ผลลัพธ์ที่ถูกต้องมากกว่า Manual Testing
c) Manual Testing มีโอกาสที่จะเกิด False Positive และ False Negative มากกว่า
d) Manual Testing จะต้องมีการอัพเดทซอฟต์แวร์ เช่น signature อย่างสม่ำเสมอ
e) Manual Testing
จะต้องใช้ผู้ที่มีความรู้และความชำนาญมากกว่า Automated Testing

121.ข้อใดเป็นวัตถุประสงค์ในการทำ Asset Audit
a) เพื่อทดสอบหาช่องโหว่ของระบบปฏิบัติการ
b) เพื่อตรวจสอบพอร์ตที่เปิดให้บริการ
c) เพื่อระบุโฮส
เครือข่ายหรือข้อมูลในองค์กรที่ควรจะปกป้องจากการถูกบุกรุก
d)
เพื่อตรวจสอบหาผู้บุกรุกทั้งภายในและภายนอกองค์กร
e) เพื่อจัดทำแผนการปฏิบัติงานในกรณีที่ระบบถูกบุกทั้งจากภายในและภายนอกองค์กร

<u>ตอนที่ 1</u> โปรดเลือกตัวเลือกที่ถูกต้องที่สุดเพียงตัวเลือกเดียว (ข้อละ 1 คะแนน)

Automated Testing

123. พิจารณาการทำ Penetration testing แบบ Black box ต่อไปนี้

หากต้องการทดสอบเจาะระบบของ BSSID หมายเลข 00:02:6F:59:94:FF ในเบื้องต้นควรใช้วิธีการใด

a) ดักจับข้อมูลแล้วใช้ aircrack-ng ในการถอดคีย์ลับที่เป็น WEP b) ดักจับข้อมูลแล้วใช้ aircrack-ng ในการถอดคีย์ลับ WPA

c) รอให้มีไคลแอนต์มาเชื่อมต่อเพื่อที่จะดู ESSID

d) ดักจับข้อมูล IVS เพื่อถอดรหัสลับ

e) ไม่สามารถทดสอบได้เนื่องจากเกิดความผิดพลาด โดยสังเกตได้จาก ESSID มีความยาว 0 ไบต์

124.ในรายงานผลการทำ Penetration Testing นั้น ผลลัพธ์ของ GAP Analysis แสดงถึงสิ่งใด

a) โอกาสที่องค์กรจะถูกบุกรุกจากภายนอกเทียบกับภายใน

b) สถานะปัจจุบันขององค์กรเทียบกับสิ่งที่องค์กรควรจะเป็นc) อัตราการเติบโตของภัยต่างๆเทียบกับจำนวนอุปกรณ์รักษาความปลอดภัยในองค์กร

d)

122. การกระทำใดที่จะเกิดใน Post-Attack Phase สำหรับการทำ Penetration Testing

a) นาย ก. ใช้ framework3 ในการทำ IIS Exploit

b) นาย ข. ใช้ NMAP ในการทำ ping sweep

c) นาย ค. ตรวจสอบหาโฟลเดอร์ที่แชร์ในระบบเครือข่าย

d) นาย ง. ใช้หลักของ Social Engineering เพื่อหาข้อมูลของผู้ใช้งาน

e) นาย จ. ลบ registry ที่เกิดจากการทดสอบเซิร์ฟเวอร์ด้วย framework3

127.เครื่องมือใดต่อไปนี้ใช้สำหรับทดสอบความปลอดภัยของ DNS

a) tshark b) dig c) smbclient

d) airreplay e) ca

128.หากต้องการตรวจสอบข้อมูลซอฟแวร์และเวอร์ชันของเมล์เซิร์ฟเวอร์ จะเลือกใช้เครื่องมือใด

a) nslookup b) nbtstat c) kismet

<u>ตอนที่ 1</u> **โปรดเลือกตัวเลือกที่ถูกต้องที่สุดเพียงตัวเลือกเดียว (ข้อละ 1 คะแนน)**

ปริมาณบุคลากรเทียบกับทรัพยากรในระบบสารสนเทศ

e) จำนวนของบุคลากรด้านไอทีเทียบกับจำนวนผู้ใช้งาน

125.ข้อใดเป็นมาตรฐานสำหรับการทำ Penetration Testing บน Web Application โดยเฉพาะ

a) ISACA b) CHECK c) OSSTMM

d) OWASP e) PIC

126.ข้อใดเป็นสูตรที่ใช้ในการหาความเสี่ยงในขั้นตอนการทำ Risk Management

a) สูตร Risk = Threat x Vulnerability

b) สูตร Risk = Threat / Vulnerability

c) สูตร Risk = Threat + Vulnerability

d) สูตร Risk = Threat – Vulnerability

e) สูตร Risk = Threat % Vulnerability

131. Which of the following statements pertaining to air conditioning for an information processing facility is correct?

a) The AC units must be controllable from outside the area.

b) The AC units must keep negative pressure in the room so that smoke and other gases are forced out of the room

c) The AC units must be in the same power source as the equipment in the room to allow for easier shutdown

d) The AC units must be dedicated to the information processing facilities

d) mail watcher e) telnet

129.The IS auditor learns that when equipment was brought into the data center by a vender, the emergency power shutoff switch was accidentally pressed and the UPS was engaged. Which of the following audit recommendations should the IS auditor suggest?

a) Relocate the shut off switch.

b) Install protective covers.

c) Escort visitors.

d) Log environmental failures.

e) None of the above

130.Which one of the following is an example of electronic piggybacking?

a) Attaching to a communication line and substituting data.

b) Abruptly terminating a dial-up or direct-connect session

c) Following an authorized user into the computer room.

d) Recording and playing back computer transactions.

e) None of the above

135. What fire suppression system can be used in computer rooms that will not damage computers and is safe for humans?

a) Water b) FM200

c) Halon

d) CO_2 e) None of the above

136. Which referring to Physical

e) None of the above

132.Which of the following questions is less likely to help in assessing physical access controls?

a) Does management regularly review the list of persons with physical access to sensitive facilities?

b) Is the operating system configured to prevent circumvention of the security software and application controls?

c) Are keys or other access devices needed to enter the computer room and media library?

d) Are visitors to sensitive areas signed in and escorted?

e) None of the above

133.Controls like guards and general steps to maintain building security, securing of server rooms or laptops, the protection of cables, and the backing up of files are some of the examples of:

a) Administrative controls

b) Logical controls

c) Technical controls

d) Physical controls

e) None of the above

134.What category of water sprinkler system is currently the most recommended water system for a computer room?

a) Dry Pipe sprinkler system

b) Wet Pipe sprinkler system

c) Pre-action sprinkler system

d) Deluge sprinkler system

e) None of the above

140.You suspect that your Windows machine has been

Security, what does Positive pressurization means?

a) The pressure inside your sprinkler system is greater than zero

b) The air goes out of a room when a door is opened and outside air does not go into the room

c) Causes the sprinkler system to go off

d) A series of measures that increase pressure on employees in order to make them more productive

e) None of the above

137.You work as the network administrator at ABC.COM A fire has devastated the server room. Fortunately you have an alternative site. What is the first process you should resume at the original site?

a) Least critical process

b) Most critical process

c) Process most expensive to maintain at an alternative site

d) Process that has a maximum visibility in the organization

e) None of the above

138.Which of the following keyloggers can't be detected by anti-virus or anti-spyware products?

a) Hardware keylogger

b) Software keylogger

c) Stealth keylogger

d) Covert keylogger

e) None of the above

139.What are the main drawbacks for anti-virus software?

a) AV software is difficult to keep up to the current revisions

b) AV software can detect viruses but can take no action

c) AV software is signature driven so new exploits are not detected

d) It's relatively easy for an attacker to change the anatomy of an attack to

compromised with a Trojan virus. When you run anti-virus software it does not pick of the Trojans. Next you run netstat command to look for open ports and you notice a strange port 6666 open. What is the next step you would do?
a) Re-install the operating system.
b) Re-run anti-virus software.
c) Install and run Trojan removal software.
d) Run utility FPORT and look for the application executable that listens on port 6666
e) None of the above

141.John wishs to install a new application onto his Windows 2008 server. He want to ensure that any application he uses has not been Trojaned. What can he do to help ensure this?
a) Compare the file's SHA-1 signature with the one published on the distribution media
b) Obtain the application via SSL
c) Compare the file's virus signature with the one published on the distribution media
d) Obtain the application from a CD-ROM disc
e) none of the above

142.Virus Scrubbers and other malware detection program can only detect items that they are aware of. Which of the following tools would allow you to detect unauthorized changes or modification of binary files on your system by unknown malware?
a) System integrity verification tools
b) Anti-virus software
bypass AV systems
e) AV software isn't available on all major operating systems platforms

d) It's relatively easy for an attacker to change the anatomy of an attack to bypass AV systems
e) AV software isn't available on all major operating systems platforms

144.Manut works primarily from home as a medical transcriptions. He just bought a brand new Dual Core Pentiium Computer with over 3 GB of RAM. He used voice recognition software is processor intensive, which is why he bought the new computer. Manut frequently has to get on the Internet to do research on what he is working on. After about two months of working on his new computer, he notices that it is not running nearly as fast as it used to. Manut used antivirus software, anti-spyware software and always keeps the computers up –to-date with Microsoft patches. After another month of working on the computer, Manut computer is even more noticeable slow. Every once in awhile, Manut also notices a window or two pop-up on his screen, but they quickly disappear. He has seen these windows show up, even when he has not been on the Internet. Manut is really worried about his computer because he spent a lot of money on it and he depend on it to work. Manut scans his through Windows Explorer and check out the file system, folder by folder to see if there is anything he can find.

<u>ตอนที่ 1</u> **โปรดเลือกตัวเลือกที่ถูกต้องที่สุดเพียงตัวเลือกเดียว (ข้อละ 1 คะแนน)**

c) properly configured gateway
d) There is no way of finding out until a new updated signature file is released
e) none of the above

143.What are the main drawbacks for anti-virus software?

a) AV software is difficult to keep up to the current revisions
b) AV software can detect viruses but can take no action
c) AV software is signature driven so new exploits are not detected

145. A malicious code that changes itself with each file infects is called a

a) Logic bomb
b) Stealth virus
c) Trojan horse
d) Polymorphic virus
e) none of the above

146. A new Worm has been released on the Internet. After investigation, you have not been able to determine of you are at risk of exposure. Management is concerned as they have heard that a number of their counterparts are being affected by the Worm. How could you determine if you are at risk?

a) Evaluate evolving environment
b) Contact your anti-virus vender
c) Discuss threat with a peer in another organization
d) wait for notification from an anti-virus vender
e) none of the above

147. A system file that has been patched numerous times becomes infected with a virus. The anti-virus software warns that disinfecting the file can damage it. What course of action should be taken?

He spends over four hours pouring over the files and folders and can't find anything but before he gives up, he notices that his computer only has about 10 GB of free space available. Since has drive is a 200 GB hard drive, Manut thinks this is very odd. Manut downloads Space Monger and adds up the sizes for all the folders and files on his computer. According to his calculations, he should have around 150 GB of free space. What is mostly likely the cause of Manut's problems?

a) Manut's computer is infected wth stealth kernel level rootkit
b) Manut's computer is infected with stealth Trojan virus
c) Manut's computer is infected with Self-Replication Worm that fills the hard disk space
d) Logic Bomb's triggered at random times creating hidden data consuming junk files
e) none of the above

149.What should a network administrator's first course of action be on receiving an e-mail alerting him to the presence of a virus on the system if a specific executable file exists?

a) Investigate the e-mail as a possible hoax with a reputable anti-virus vender

b) Immediately search for and delete the file if discovered

c) Broadcast a message to the entire

a) Replace the file with the original version from master media
b) Proceed with automated disinfection
c) Research the virus to see of it is benign
d) Restore an uninfected version of the patched file from backup media
e) none of the above

148. One of your users calls to state the their computer is acting unusual. You go to investigate and find there is an unauthorized program installed on this computer. You examine the network and find that this program has replicated itself to other machines in the network, without the input of the user. What type of program is in the network?

a) The program is a Worm b) The program is a Virus
c) The program is a Bug d)The program is a Trojan horse
e) The program is a Macro

153.You have been asked to investigate the possibility of computer fraud in the finance department of a company. It is suspected that a staff member has been committing finance fraud by printing cheques that have not been authorized. You have exhaustively searched all data files on a bitmap images of the target computer, but have found no evidence. You suspect the files may not have been saved. What should you examine next in this case?

a) The registry b) The swapfile
c) The recycle bin d) The organization to alert users to the presence of a virus

d) Locate and download a patch to repair the file

e) none of the above

150.What is used by anti-virus software to detect unknown viruses?

a) Zero-day algorithm is used to detect unknown viruses

b) Heuristic analysis is used to detect unknown viruses

c) Random scanning is used to detect unknown viruses

d) Quarantining is used to detect unknown viruses

e) none of the above

151.Which types of attachments should be filters from e-mails to minimize the danger of viruses?

a) Test files b) Image files c) Sound files
d) Executable files e) none of the above

152. A manager reports that users are receiving multiple emails from the account of a user who no longer works for the company. Which of the following would be the best way to determine whether the emails originated internally?

a) Look at the source IP address in the SMTP header of the emails
b) Reply to the email and check the destination email address
c) Look at the from line of the emails

<u>ตอนที่ 1</u> **โปรดเลือกตัวเลือกที่ถูกต้องที่สุดเพียงตัวเลือกเดียว (ข้อละ 1 คะแนน)**

metadata e) none of the above

154.What is the act of willfully changing data, using fraudulent input or removal of controls called?

a) Data diddling b) Data contaminating c) Data capturing d) Data trashing e) none of the above

155.Separation of duties is valuable in deterring

a) DoS b) External intruder c) Fraud

d) Trojan horse e) none of the above

156.What principle requires that for particular sets of transactions, no single individual bee allowed to execute all transactions within the set?

a) Use of rights b) Balance of power
c) Separation of duties d) Fair use
e) none of the above

157.What is the company benefit, in terms of risk, for people taking a vacation of a specified minimum length?

a) Reduces stress levels, thereby lowering insurance claims

b) Improves morale, thereby decreasing errors

c) Increase potential for discovering frauds

d) Review anti-virus logs on the former employee's computer
e) none of the above

158. What are the benefits of job rotation?

a) Cross training to employees

b) Trained backup in case of emergencies

c) Protect against fraud

d) All of the choices

e) none of the above

159. As per the guidelines in the ISO Security Policy standard, what is the purpose of the section on Personnel Security?

a) The objectives of this section are to control access to information, to prevent unauthorized access to information systems, to ensure the protection of networked services, and to prevent unauthorized computer access

b) The objectives of this section are to avoid breaches of any criminal or civil law, statutory, regulatory or contractual obligations and of any security requirements, and to ensure compliance of systems with organizational security policies and standards

c) The objectives of this section are to

<u>ตอนที่ 1</u> **โปรดเลือกตัวเลือกที่ถูกต้องที่สุดเพียงตัวเลือกเดียว (ข้อละ 1 คะแนน)**

d) Reduces dependence on critical individuals

e) none of the above

160.Security Service ที่ดี ต้องรับประกันเรื่องใดบ้าง

a) Confidentiality b) Integrity c) Availability

d) a และ b เท่านั้น e) a และ b และ c

161. สิ่งแรกที่ควรทำให้การวาง Security Services คือ

a) user requirement analysis b) risk analysis

c) network system analysis d) a และ b เท่านั้น

e) b และ c เท่านั้น

162. Risk analysis ประกอบด้วย

a) assets b) threats c) managements

d) a และ b เท่านั้น e) b และ c เท่านั้น

163. ข้อใดคือจุดประสงค์ของการทำ Hardening

provide management direction and support for information security

d) The objectives of this section are to reduce risks of human error, theft, fraud or misuse of facilities, to ensure that users are aware of information security threats and concerns, and are equipped to support the corporate security policy in the course of their normal work, to minimize the damage from security incidents and malfunctions and learn from such incidents

e) The objectives of this section are to maintain appropriate protection of corporate assets and to ensure that information assets receive an appropriate level of protection

165. ในการวางแผนออกแบบ network security architecture จะต้องมีการสำรวจทรัพย์สินทาง IT ที่องค์กรมีอยู่ เพื่อที่จะ

a). รู้ว่า จะต้องวางแผนได้ถูกต้องอย่างไร

b). รู้ว่า เมื่อไรแผนเสร็จสมบูรณ์

c). รู้ว่า ออกแบบแผนได้ดี

d). b และ c เท่านั้น

<u>ตอนที่ 1</u> โปรดเลือกตัวเลือกที่ถูกต้องที่สุดเพียงตัวเลือกเดียว (ข้อละ 1 คะแนน)

a. การป้องกัน Kernel, Hardware และ Memory ต่างๆจากโปรแกรมที่ทำการประมวลผลอยู่ในอุปกรณ์นั้นๆ

b. การจำกัด Services และ Activities ต่างๆบนอุปกรณ์นั้นๆ

c. การปิดช่องโหว่ รวมไปถึงการ Update Patch เพื่อแก้ไขจุดบกพร่องต่างๆของอุปกรณ์นั้นๆ

d. ไม่มีข้อใดถูกต้อง

e. ถูกทุกข้อ

164. การมี network security architecture ที่ดี จะทำให้องค์กร

a.) ลดความซับซ้อนในการบริหารจัดการ

b.) เลือกใช้เทคโนโลยีที่เหมาะสมได้ง่ายขึ้น

c.) เลือกใช้เทคโนโลยี โดยไม่ผูกติดกับยี่ห้อ

d.) b และ c เท่านั้น

e.) a และ b และ c

169. การป้องกัน data center จากอัคคีภัยที่ดี

e). a และ b และ c

166. พื้นฐานสุดของระบบเครือข่ายที่ปลอดภัยต้องสามารถ

a). แยกส่วนที่เก็บข้อมูลสำคัญออกได้

b). ป้องกันการเข้าถึงข้อมูลสำคัญ จากผู้ที่ไม่มีสิทธิ

c). ป้องกันความเสียหายของข้อมูลสำคัญ

d). b และ c เท่านั้น

e). a และ b และ c

167. ระบบเครือข่ายที่มีความปลอดภัยระดับสูงสุดมีขีดความสามารถ

a). ปรับเปลี่ยนระดับความป้องกันของเครือข่ายจากการบุกรุกได้เอง

b). บริหารจัดการตัวตน (identity management)

c). บริหารจัดการสิทธิการเข้าถึงข่าวสาร (information rights management)

d). b และ c เท่านั้น

e). a และ b และ c

168. สิ่งใดที่ก่ออันตรายใน Data center

a). ควันไฟ

b). ไฟไหม้

<u>ตอนที่ 1</u> โปรดเลือกตัวเลือกที่ถูกต้องที่สุดเพียงตัวเลือกเดียว (ข้อละ 1 คะแนน)

a). ติดตั้งระบบ Microsoft System Center Data Protection Manager

b). ติดตั้งระบบตรวจจับควันไฟ

c). ติดตั้งระบบตรวจจับเปลวไฟ

d). b และ c เท่านั้น

e). a และ b และ c

170. หากเกิดไฟไหม้ใน data center สิ่งที่ได้รับความเสียหายมากที่สุดคือ

a). network administrators b). servers

c). ข้อมูล d). b และ c เท่านั้น

e). a และ b และ c

171. data center ที่ดี ควรมีลักษณะ

a). แยกตัวออกจากส่วนอื่นๆของอาคาร

b). ใช้ระบบป้องกันไฟของอาคารหลักเป็นด่านป้องกันด่านแรก

c). มี main switch ที่สามารถตัดไฟ UPS ได้โดยง่าย เพื่อป้องกันไฟชอร์ตเจ้าหน้าที่

d). b และ c เท่านั้น

e). a และ b และ c

c). ระบบน้ำดับไฟ

d). b และ c เท่านั้น

e). a และ b และ c

174. ปัญหาของ tape backup คือ

a). เสียเวลาในการ backup b). เสียเวลาในการ recovery

c). เสียเวลาในการค้นหาข้อมูล d). b และ c เท่านั้น

e). a และ b และ c

175. จุดเด่นของ tape backup คือ

a). ราคาถูก b). ใช้งานง่าย c). มีความเชื่อถือได้ระดับหนึ่ง

d). b และ c เท่านั้น e). a และ b และ c

176. ปัญหาของการ backup ข้อมูลไปยัง secondary data center คือ

a). ยิ่งใกล้ ยิ่งแพง b). ยิ่งไกล ยิ่งเชื่อถือไม่ได้

c). คนภายนอกเข้าถึงข้อมูล backup ได้ง่าย d). b และ c เท่านั้น

e). a และ b และ c

177. ISO18028-2 เน้นเรื่อง network security

ตอนที่ 1 โปรดเลือกตัวเลือกที่ถูกต้องที่สุดเพียงตัวเลือกเดียว (ข้อละ 1 คะแนน)

172.ระบบสำรองข้อมูลที่ดี ใน data center

a). อยู่ใกล้ server หลักมากที่สุด b). สำรองข้อมูลโดยอัตโนมัติ

c). สำรองข้อมูลที่ระดับ byte d). b และ c เท่านั้น

e). a และ b และ c

173. ระยะทางใกล้ main site ที่สุดของ backup data center คือ

a). 100 เมตร b). 500 เมตร c). 2,000 เมตร

d). 10 กิโลเมตร e). 30 กิโลเมตร

180.ระบบบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศใช้กระบวนการใดในการดำเนินการกำหนด ลงมือปฏิบัติ ดำเนินการ เฝ้าระวัง ทบทวน บำรุง รักษาและปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัย

a. C-D-M-A
b. P-D-C-A
c. D-C-A-R
d. S-A-S-C
e. F-I-F-O

181.ช่องโหว่ของระบบเรียกว่าอะไร

a. Patch

ที่ระดับ

a). core switch b). end-to-end network

c). infrastructure technology d). b และ c เท่านั้น

e). a และ b และ c

178. ควรมีการตรวจสอบ network security architecture ทุกๆระยะเวลา

a). 7 วัน b). 1 เดือน c). 3 เดือน

d). 1 ปี e). 3 ปี

179.ข้อใดเป็นโปรแกรมเสริมบนโปรแกรม Antivirus เพื่อให้สามารถตรวจจับไวรัสทางเมลล์ได้ดียิ่งขึ้น

a. Anti-Spam
b. Mail Gateway
c. Mail filtering
d. Content Filtering
e. Mail box

185.ผู้บริหารของบริษัท ก. มีความจำเป็นต้องเดินทางไปต่างประเทศบ่อย

<u>ตอนที่ 1</u> โปรดเลือกตัวเลือกที่ถูกต้องที่สุดเพียงตัวเลือกเดียว (ข้อละ 1 คะแนน)

b. Firmware

c. Vulnerability

d. Confidential

e. Microsoft Windows

182.ข้อใดเป็นไวรัสที่โจมตีผ่านช่องโหว่ของระบบ

a. Harakit

b. Conflicker

c. BackDoor.Tdss

d. Sality

e. All are correct

183.โปรแกรมในข้อใดทำการ execute ไวรัสจาก USB Drive เมื่อเสียบเข้ากับเครื่องคอมพิวเตอร์

a. Desktop.ini

b. Auntorun.inf

c. Recycler

d. System Volume Information

e. None of above

184.ไฟล์นามสกุลข้อใดที่ไม่สามารถเป็นไวรัสหรือแพร่ไวรัสได้

a) EXE

b. COM

c. VBS

แต่ต้องการใช้งานแอพพลิเคชั่นภายในองค์กร การเชื่อมต่อวิธีใดเหมาะสมที่สุด

a) Roaming Mobile

g. VPN Access

c) ADSL Router

d) Internet Access

e) Air Card

186.บริษัท ข. ต้องการทำธุรกิจในลักษณะของ E-Commerce ซึ่งแอพพลิเคชั่นที่ใช้งานจำเป็นต้องเชื่อมต่อมาจากอินเตอร์เน็ต ถ้าต้องการให้ได้ประสิทธิภาพในการใช้งานสูงในขณะที่ยังคงความมั่นคงปลอดภัยของข้อมูลไว้ เราควรวางเครื่องแม่ข่ายที่ตำแหน่งใดจึงจะเหมาะสม

a. ภายใน DMZ ของ Firewall

b. หลังจาก Internet Router

c. ภายใน Internal Data Center

d. หลังจาก Reverse Proxy

e. ก่อนเข้า Core Switch

187.บริษัท ค. โดน Hacker โจมตี Web Server ผ่านทาง protocol HTTP พอร์ต 80 จะป้องกันการโจมตีดังกล่าวได้อย่างไร

a. set policy Firewall ให้ปิดพอร์ต 80

b. ตั้ง IPS เพื่อดักจับการโจมตี

c. set routing บน Internet Router ให้ส่งไปที่อื่น

d. เปลี่ยนการใช้งานของ Web Server เป็นพอร์ตอื่น

<u>ตอนที่ 1</u> **โปรดเลือกตัวเลือกที่ถูกต้องที่สุดเพียงตัวเลือกเดียว (ข้อละ 1 คะแนน)**

d. TXT

e. None of above

190.คุณสมศรีไปซื้ออุปกรณ์ IPS มาเพื่อติดตั้งใช้งานเพื่อให้ระบบเครือข่ายที่ตนเองดูแลอยู่มีความมั่นคงปลอดภัยมากขึ้น หลังจากนำมาติดตั้งตามคำแนะนำในคู่มือแล้ว พบว่าผู้ใช้งานไม่สามารถเข้าใช้งานระบบบัญชีได้ ในขณะที่ระบบอื่นๆ ใช้งานได้ตามปกติ เมื่อถอดอุปกรณ์ IPS ออกก็สามารถใช้งานได้ตามปกติ คิดว่าปัญหาดังกล่าวน่าจะเกิดจากสาเหตุใด

a. อุปกรณ์ IPS ที่ซื้อมาเสีย

b. เครื่องแม่ข่ายที่ติดตั้งระบบบัญชีมีปัญหา

c. เครื่องของผู้ใช้งานมีปัญหา

d. ระบบเครือข่ายมีปัญหา

e. การปรับแต่ง policy ของ IPS มีปัญหา

191.คุณสมศักดิ์กำลังจะติดตั้งระบบเครือข่ายไร้สาย (Wireless LAN) ภายในบริษัท และต้องการให้เกิดความมั่นคงปลอดภัยของข้อมูลด้วยเพราะบริษัทของคุณสมศักดิ์อยู่ในอาคารสำนักงานให้เช่า ซึ่งมีอีกหลายบริษัทมาเช่าใช้งานอยู่ร่วมกัน คุณสมศักดิ์ควรทำอย่างไร

e. เปลี่ยน password เข้าใช้งาน server ทุกเดือน

188.ถ้าต้องการเลือกวิธีในการ encryption เราควรเลือกแบบไหนถึงจะมีความมั่นคงปลอดภัยที่สุด

a) DES

b) 3DES

c) AES

d) 3AES

e) ZES

189. เครื่องแม่ข่ายที่ใช้ระบบปฏิบัติการ Microsoft Windows ของคุณสมชายโดน Hacker เข้ามาก่อกวนจนไม่สามารถให้บริการกับผู้ใช้งานได้ เรียกได้ว่าคุณสมชายกำลังโดนโจมตีด้วยวิธีการใดอยู่

a) DDOS b) MSDOS
c) D-Flood

d) MS-Flood e) MS-Jail Break

194.คุณเป็นพนักงานในร้านสะดวกซื้อแห่งหนึ่งทำหน้าที่เกี่ยวกับการเช็คสต๊อกสินค้าที่เข้ามากับสินค้าขายไปอยู่มาวันหนึ่งคุณพบว่าปริมาณสินค้าที่ขายไปกับยอดจำหน่ายสินค้าที่ปรากฏในข้อมูลของเครื่องเก็บเงินไม่ตรงกัน และต่อมาจึงพบว่าปัญหานั้นเกิดมาจากเพื่อนร่วมงานของคุณที่ทำหน้าที่เก็บเงินได้ดัดแปลงคอมพิวเตอร์ของเครื่องเก็บเงินให้คิดราคาสินค้าผิดโดยคิดราคาน้อยกว่าปกติ เช่นสินค้าราคาจริง 100 บาทแต่เครื่องเก็บเงินจะคิดราคาแค่ 50 บาท เมื่อลูกค้าจ่ายเงินเท่าราคาจริงจะทำให้พนักงานคนนั้นได้เงินส่วนต่างไป คุณจะแก้ไขปัญหานี้อย่างไร

<u>ตอนที่ 1</u> **โปรดเลือกตัวเลือกที่ถูกต้องที่สุดเพียงตัวเลือกเดียว (ข้อละ 1 คะแนน)**

a) Disable SSID Broadcast b) Lock MAC Address

c) Enable Encryption d) ทำทุกข้อ

e) ไม่ต้องใช้งาน Wireless LAN

192.บริษัท จ.
มีความต้องการที่จะให้มีการระบุตัวตนผู้ใช้งาน รวมถึงตรวจสอบการอัพเดท patch ของ OS และ Anti-Virus Software
ให้ทันสมัยก่อนการเข้าใช้งานระบบ
เพื่อให้ระบบเครือข่ายมีความปลอดภัย
เทคโนโลยีใดที่น่าจะเหมาะสมกับความต้องการนี้ที่สุด

a) Firewall b) NAC c) Authentication

d) Patch Management e) VPN

193.หากคุณพบว่าเวบไซท์ e-banking ของธนาคารแห่งหนึ่งที่คุณเข้าใช้บริการมีช่องโหว่ที่ทำให้สามารถเจาะระบบเข้าไปขโมยข้อมูลของผู้ใช้งานคนอื่นได้ คุณคิดว่าจะปฏิบัติเช่นไร

a. deface หน้าเวบเพจเพื่อเป็นการเตือนธนาคาร

b. อาศัยช่องโหว่นั้นเพื่อขโมยข้อมูลของผู้ใช้งานอื่นและนำเงินมาใช้เป็นของตัวเอง

c)
โทรไปต่อว่าธนาคารนั้นๆว่าเวบไซท์ไม่มีความปลอดภัยและจะไม่ใช้บริการใดๆของธนาคารแห่งนี้อีก

d)
โทรไปแจ้งช่องโหว่ที่พบกับทางธนาคารเพื่อให้รีบ

a. บอกผู้จัดการร้านว่าพนักงานเก็บเงินยักยอกเงินไปและให้ไล่พนักงานคนนั้นออกทันที แต่ไม่บอกว่าเครื่องเก็บเงินโดนแก้ไขเพื่อที่คุณจะได้ใช้มันยักยอกเงินต่อไป

b)
บอกพนักงานเก็บเงินคนดังกล่าวว่าหากไม่ยอมแบ่งเงินให้คุณครึ่งนึง คุณจะนำเรื่องไปฟ้องผู้จัดการร้าน

c)
บอกผู้จัดการร้านว่าเครื่องเก็บเงินโดนแก้ไขให้คิดจำนวนเงินผิด และเสนอแนวทางแก้ไขหากเป็นไปได้

d)
บอกพนักงานเก็บเงินคนดังกล่าวให้สอนวิธีแก้ไขเครื่องเก็บเงินแก่คุณ
จากนั้นลาออกไปทำงานเป็นพนักงานร้านสะดวกซื้ออีกร้านหนึ่งและแก้ไขเครื่องเก็บเงินของร้านนั้นเพื่อจะได้เงินมาอย่างง่ายดาย

e)
ทำเป็นไม่สนใจและปล่อยให้ผู้จัดการเป็นคนค้นพบปัญหาด้วยตัวเองเพื่อกันความระหองระแหงระหว่างเพื่อนร่วมงาน

195.นายสมชายเป็นผู้ให้คำปรึกษาเกี่ยวกับระบบความปลอดภัยเครือข่าย
มีบริษัทแห่งหนึ่งต้องการจ้างนายสมชายไปทำ penetration testing
ระบบเครือข่ายที่ใช้งานอยู่ว่ามีความปลอดภัยมากน้อยแค่ไหน โดยเสนอเงินเป็นจำนวน 1,000,000 บาท
หากแต่เมื่อนายสมชายได้สอบถามรายละเอียดแล้วกับพบว่าระบบเครือข่ายของบริษัทมีเพียง router สำหรับต่อกับ internet ภายนอก และมีเครื่อง Web server กับ Database
เพียงเครื่องเดียวเท่านั้นซึ่งมีมูลค่าทรัพย์สินและข้อมูลเพียง 100,000 บาท นายสมชายควรจะทำอย่างไร

a)
ชี้แจงให้ลูกค้าเข้าใจว่ากำลังจะจ่ายเงินสำหรับค่าความปลอดภัยเกินกว่ามูลค่าของทรัพย์สินซึ่งเป็นการไม่เหมาะที่จะทำ

ดำเนินการแก้ไข

e) เลิกใช้บริการ e-banking
เป็นการถาวรเพื่อความปลอดภัย

196. นายสมบูรณ์เป็น Network Engineer ในบริษัทที่เป็น System Integrator แห่งหนึ่ง ทุกครั้งที่ไปติดตั้งอุปกรณ์เครือข่ายให้ลูกค้าไม่ว่าจะเป็น Router, Switch , Firewall , IDS/IPS นายสมบูรณ์จะสร้าง user account ลับอีกอันหนึ่งสำหรับตนเองไว้เพื่อความสะดวกในการเข้ามาแก้ปัญหาอุปกรณ์จากภายนอกได้โดยไม่ต้องขออนุญาตลูกค้าให้ยุ่งยากและสามารถแก้ปัญหาได้อย่างรวดเร็ว คุณคิดว่านายสมบูรณ์ทำถูกหรือไม่

a. ถูก เพราะ ถ้าไม่มี user account ที่สามารถ login เข้าไปยังอุปกรณ์ได้เลยจะทำให้แก้ปัญหาได้ช้า

b. ผิด เพราะ อุปกรณ์เหล่านั้นเป็นทรัพย์สินของลูกค้า นายสมบูรณ์จึงไม่มีสิทธิ์ในการเข้าถึงอุปกรณ์โดยลูกค้ายังไม่ได้อนุญาต

c. ถูก เพราะ อุปกรณ์เหล่านั้นคนติดตั้งควรจะต้องทราบ username / password อยู่แล้ว

d. ผิด เพราะ นายสมบูรณ์ควรเป็นเพียงคนเดียวที่มี user account โดยไม่ต้องบอกลูกค้าและไม่ให้ลูกค้าเข้ามายุ่งเกี่ยวกับตัวอุปกรณ์ด้วย

e. ถูก เพราะ อุปกรณ์ Router , Switch , Firewall จะต้องมี username / password เหมือนกันทุกอุปกรณ์เสมอ

จากรูปใช้ในการตอบคำถาม ข้อ 197-199

b)
รีบตกลงรับงานทันทีเนื่องจากเป็นงานที่ง่ายและให้ค่าตอบแทนสูงซึ่งนานๆจะมีสักที

c) ไม่รับงานเพราะง่ายเกินไป
ไม่เหมาะสมกับระดับความรูของตน

d)
รับงานมาทำจากนั้นรีบเสนอให้ลูกค้าซื้ออุปกรณ์รักษาความปลอดภัยเครือข่ายต่างๆเพิ่มขึ้นอีกหลายอย่างเพื่อความปลอดภัย เช่น Firewall , IDS/IPS

e)
แนะนำให้เพื่อนมาทำงานนี้ด้วยกันเพื่อแสดงความมีน้ำใจ

198. ถ้าองค์กรมีการให้บริการ Web Service แก่ผู้ใช้งานทั้งภายในและภายนอกองค์กร ควรจะทำการติดตั้ง Web Server ไว้ที่ Zone ใดจึงจะเหมาะสมที่สุด

a. Internet Zone

b. DMZ Zone

c. Server Zone

d. Internal Zone

e. ไม่มีข้อใดถูก

199. ถ้ามีการติดตั้ง Antivirus ให้กับเครื่องคอมพิวเตอร์ทุกเครื่องที่อยู่ใน Internal Zone ข้อใดต่อไปนี้ถูกต้อง

a) เครื่องคอมพิวเตอร์ทุกเครื่องใน Internal Zone จะไม่มีวันติดไวรัสอีก

b) เครื่องคอมพิวเตอร์ทุกเครื่องใน Internal Zone จะไม่มีวันแพร่กระจายไวรัสได้อีก

c)

ตอนที่ 1 โปรดเลือกตัวเลือกที่ถูกต้องที่สุดเพียงตัวเลือกเดียว (ข้อละ 1 คะแนน)

และเลือกคำตอบที่ถูกต้องที่สุด

197. จากรูปถ้าต้องการให้ผู้ใช้ (User) ซึ่นั่งอยู่ที่ Internal Zone สามารถใช้งาน Internet (Internet Surfing) จะต้องกำหนดนโยบาย (Policy) ที่ไฟล์วอล ให้ทำการเปิด Port ปลายทางอะไร

a. Port 65 b) Port 70 c) Port 75

d) Port 80 e) Port 85

อาจจะเกิดการติดไวรัสและแพร่กระจายของไวรัสได้หากไม่มีการอัพเดท Antivirus

d) ข้อ a, b ถูก

e) ไม่มีข้อใดถูก

200.ข้อใดต่อไปนี้คือข้อดีของการติดตั้ง IDS ไว้ข้างหน้า Server Zone

a. IDS
สามารถทำการตรวจจับการบุกรุกที่เจาะผ่านไฟล์วอลมาได้

b. IDS
สามารถตรวจจับกิจกรรมที่ไม่ได้รับอนุญาติของผู้ใช้งานภายในองค์กร (Internal Zone)

c. IDS
สามารถทำการเก็บรวบรวมสถิติเกี่ยวกับความพยายามหรือการโจมตี
และนำข้อมูลไปทำการวิเคราะห์ภัยคุกคามที่อาจจะเกิดขึ้นกับ Server Zone ได้

d. a, b ถูก

e. a, b, c ถูก

<u>ตอนที่ 1</u> โปรดเลือกตัวเลือกที่ถูกต้องที่สุดเพียงตัวเลือกเดียว (ข้อละ 1 คะแนน)

<u>ตอนที่ 1</u> โปรดเลือกตัวเลือกที่ถูกต้องที่สุดเพียงตัวเลือกเดียว (ข้อละ 1 คะแนน)
