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

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

1. SANS Institute ได้กล่าวถึงขั้นตอนแรกของการจัดการเหตุการณ์ที่เกิดขึ้นอย่างมีประสิทธิภาพ คือข้อใด

   a. Preparation
   b. Reading
   c. Monitor
   d. Containment
   e. Recovery

2. CSIRT ย่อมาจาก

   a. Computer System Information Rescue Team
   b. Computer Security Information Rescue Team
   c. Computer Security Information Response Team
   d. Computer System Information Response Team
   e. ไม่มีข้อใดถูกต้อง

3. เครื่องมือใดที่สามารถช่วยให้รับรู้เหตุการณ์ที่เกิดขึ้นในระบบเทคโนโลยีสารสนเทศได้อย่างรวดเร็ว

   a. IDPS
   b. DIPS
   c. SIEM
   d. MISE
   e. ไม่มีข้อใดถูกต้อง

ข้อความต่อไปนี้ ใช้ตอบคำถามสำหรับข้อ 6 – 10

นาย ก. เป็นพนักงานแผนกเทคโนโลยีสารสนเทศ มีหน้าที่ในการดูแลระบบสารสนเทศของบริษัทฯให้สามารถทำงานได้ตามปกติ

6. นาย ก. ได้รับการแจ้งทางโทรศัพท์จากพนักงานว่าเครื่องตนเองติดไวรัส นาย ก. จึงได้รีบเข้าไปที่เครื่องของพนักงานท่านนั้นทันที ข้อใดถูกต้องที่สุด

   a. บริษัทฯ ไม่มีระบบการจัดการเหตุการณ์ที่เกิดขึ้นที่ดี
   b. นาย ก. ติดตั้งระบบป้องกันไวรัสให้พนักงานไม่ดี
   c. พนักงานใช้งานเครื่องของตนไม่ดี
   d. ถูกทุกข้อ
   e. ไม่มีข้อใดถูกต้อง

7. เมื่อนาย ก. รู้ว่ามีไวรัสระบาดในระบบ นาย ก. จึงรีบเข้าไปปรับแต่งอุปกรณ์ Firewall ทันที ข้อใดถูกต้องที่สุด

   a. นาย ก. ทำได้ดีแล้ว ในการที่จะหยุดไวรัสไม่ให้ระบาด
   b. นาย ก. ทำไม่ถูกต้อง และรีบดำเนินการเร็วไป
   c. นาย ก. ทำไม่ถูกต้อง เพราะควรจะไปแก้ไขที่ Anti Virus Server
   d. ถูกทุกข้อ

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

4. วงจรในการรับมือเหตุการณ์ที่เกิดขึ้นคือ

   a. AIRP

   b. PAIR

   c. RAPI

   d. IAPR

   e. ไม่มีข้อใดถูกต้อง

5. ในการตรวจสอบข้อมูลจากเหตุการณ์ที่เกิดขึ้น สามารถตรวจสอบข้อมูลได้จาก

   a. Proxy Server

   b. Firewall

   c. Intruder Protection System

   d. ถูกทุกข้อ

   e. ไม่มีข้อใดถูกต้อง

9. หลังจากที่นาย ก. ปิดระบบทั้งหมดและทำให้ไวรัสหยุดทำงาน แล้ว นาย ก. ควรจะทำอย่างไร

   a. เปิดเครื่อง server หลักก่อน

   b. เปิดเครื่อง client ที่คิดว่าสะอาดก่อน

   c. เปิดเครื่อง server ที่คิดว่าสะอาดก่อน

   d. ถูกทุกข้อ

   e. ไม่มีข้อใดถูกต้อง

   e. ไม่มีข้อใดถูกต้อง

8. หลังจากที่ไวรัสได้ระบาดไปแล้ว นาย ก. ยังหาหนทางให้ไวรัสหยุดไม่ได้ นาย ก. ตัดสินใจ ป้องกันปัญหาที่เกิดขึ้นกับข้อมูลของระบบที่จะเสียหาย จึงตัดสินใจหยุดระบบสารสนเทศเพื่อให้ไวรัสไม่แพร่กระจายต่อไป ข้อใดถูกต้องที่สุด

   a. นาย ก. ทำไม่ถูกต้อง เพราะทำให้ระบบสารสนเทศทั้งหมดหยุดทำงาน

   b. นาย ก. ทำถูกต้อง เพราะทำให้ไวรัสไม่ทำลายข้อมูลในระบบ

   c. นาย ก. ทำไม่ถูกต้อง เพราะนาย ก. ไม่มีกระบวนการจัดการเหตุการณ์อย่างถูกวิธี

   d. ถูกทุกข้อ

   e. ไม่มีข้อใดถูกต้อง

14. ข้อใดถูกต้องที่สุดสำหรับสารที่ใช้ดับไฟไหม้ที่เกิดจากอุปกรณ์ไฟฟ้า

   a. Halon

   b. Soda acid

   c. Nitrogen

   d. Carbon Dioxide

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

10. บริษัทฯ ได้ทราบถึงความเสียหายที่เกิดขึ้นกับระบบ ที่ นาย ก. ได้ทำการปิดระบบทั้งหมด บริษัทฯ ควรทำอย่างไร

a. ให้รางวัล นาย ก. ในการป้องกันไวรัสไม่ให้ลุกลาม
b. ลงโทษ นาย ก. ที่ทำให้ระบบหยุดทำงาน
c. ไม่ทำอะไร นาย ก. เพราะนาย ก. ทำตามหน้าที่
d. ถูกทุกข้อ
e. ไม่มีข้อใดถูกต้อง

11. สิ่งใดถูกต้องที่สุดในการป้องกันให้เกิดความมั่นคงทางกายภาพ

a. ติดตั้งประตูไม่ให้ผู้บุกรุกเข้ามา
b. ตรวจสอบลายนิ้วมือก่อนเข้าห้อง
c. ตรวจสอบรายชื่อผู้เข้าห้อง
d. ถูกเฉพาะข้อ a และ b
e. ถูกทุกข้อ

12. ความสูงของรั้วที่สามารถขัดขวางบุคคลที่ตั้งใจบุกรุกได้ ต้องมีความสูงเป็นอย่างน้อยเท่าใด

a. 1.9 เมตร
b. 2.4 เมตร
c. 3.5 เมตร
d. 4.6 เมตร
e. 5.7 เมตร
e. Foam

15. ข้อใดถูกต้องที่สุด สำหรับระบบความมั่นคงปลอดภัยของห้องคอมพิวเตอร์ในศูนย์คอมพิวเตอร์

a. กำแพงของห้องไม่ควรเป็นกำแพงเดียวกับอาคาร
b. ไม่ควรใกล้สายไฟ
c. ไม่ควรใช้กระจกเป็นกำแพง
d. ไม่มีข้อใดถูกต้อง
e. ถูกทุกข้อ

16. รั้วที่มีความแข็งแรงสามารถป้องกันให้ปลอดภัยในระดับกลางจนถึงสูง ต้องใช้เหล็กมาถักทอกันจนเป็นผืนรั้วนั้น ขนาดช่องตารางเล็กๆที่เหล็กมาถักทอกันเป็นรั้วนั้น ขนาดของช่องที่เล็กที่สุดต้องมีขนาดไม่เกินเท่าใด

a. 1x1 นิ้ว
b. 1.5x1.5 นิ้ว
c. 2x2 นิ้ว
d. 2.5x2.5 นิ้ว
e. ไม่มีข้อใดถูกต้อง

17. ข้อใดที่ CCTV ไม่สามารถทำได้

a. Detection
b. Recognition
c. Identification

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

13. สาเหตุสำคัญที่สุดที่ทำให้ตึก world trade ถล่ม ในเหตุการณ์ วันที่ 11 เดือนกันยายน พ.ศ. 2544

a. ตัวเครื่องบินแข็งแรงกว่าตัวตึก
b. จำนวนคนที่อยู่ในตึก
c. โครงสร้างโลหะของตึก
d. ไม่มีข้อใดถูกต้อง
e. ถูกทุกข้อ

19. ข้อใดถูกต้องที่สุด

a. ไม่ควรมี master key เพราะทำให้มีโอกาสถูกบุกรุกได้
b. กล้องวงจรปิด ไม่สามารถจับคนร้ายได้
c. ท่อน้ำ ไม่เกี่ยวข้องกับความมั่นคงทางด้านกายภาพ
d. ไม่มีข้อใดถูกต้อง
e. ถูกทุกข้อ

20. ข้อใดถูกต้องที่สุด

a. ระบบจ่ายไฟสำรองเป็นส่วนหนึ่งของความมั่นคงทางด้านกายภาพ
b. ระบบตรวจสอบควันไฟเป็นส่วนหนึ่งของความมั่นคงทางด้านกายภาพ
c. การดูแลคอมพิวเตอร์พกพา (Laptop)
d. ไม่มีข้อใดถูกต้อง
e. ถูกทุกข้อ

18. ข้อใดที่สายใยแก้วนำแสง (Fiber Optic Cable) สามารถป้องกันได้

a. ป้องกันการรั่วของคลื่นแม่เหล็กได้
b. ป้องกันการสูญเสียข้อมูลจากการส่งได้
c. ป้องกันการดึงข้อมูลจากสายใยแก้วได้
d. ไม่มีข้อใดถูกต้อง
e. ถูกทุกข้อ

23. สิ่งที่สามารถก่อให้เกิดอันตรายต่อระบบสารสนเทศหมายถึง

a. ความเสี่ยง
b. ภัยคุกคาม
c. ช่องโหว่
d. จุดอ่อน
e. ผลกระทบของเหตุการณ์ที่เกิด

24. ข้อใดเป็นสิ่งแรกในการป้องกันด้านความลับ(Confidentiality) ของข้อมูล

a. การติดตั้ง firewall
b. การติดตั้งการเข้ารหัส
c. การระบุสารสนเทศที่มีความสำคัญ
d. การพิสูจน์ตัวตนในการเข้าถึงของผู้ใช้งานระบบ
e. การตรวจสอบสิทธิในการเข้าถึงของผู้ใช้งานระบบ

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

เป็นส่วนหนึ่งของความมั่นคงทางด้านกายภาพ

d. ไม่มีข้อใดถูกต้อง

e. ถูกทุกข้อ

21. ในการจัดการความเสี่ยง ต้องเริ่มต้นจากการกำหนดระดับความสำคัญของทรัพย์สิน ซึ่งจะคำนึงถึงสิ่งใดเป็นหลัก

a. ประเภทของผู้เข้าถึงข้อมูล ได้แก่ พนักงาน พนักงานชั่วคราว และลูกค้า

b. การประเมินระดับความเสี่ยง

c. การประเมินระดับความเสี่ยงและการป้องกันที่ปิดไป

d. การควบคุมการเข้าถึงที่ใช้ในการป้องกันข้อมูล

e. Confidentiality, Integrity และ Availability

22. ผลจากโอกาสที่เกิดของภัยคุกคามที่มีผลกระทบต่อระบบสารสนเทศ เรียกว่า

a. ภัยคุกคาม

b. ความเสี่ยง

c. ช่องโหว่

d. จุดอ่อน

e. ผลกระทบของเหตุการณ์ที่เกิด

28. ในกรณีที่บริษัทต้องการจะทำการป้องกันทรัพย์สินที่มีมูลค่า 1,000,000 บาท จากภัยคุกคามที่มีโอกาสเกิดขึ้น 1 ครั้งในทุก 5 ปี และค่าความเสียหายคิดเป็น 40% ของมูลค่าทรัพย์สิน

25. ข้อใดอธิบายถึงความหมายของการบริหารความเสี่ยง (Risk Management) ได้ดีที่สุด

a. กระบวนการในการกำจัดความเสี่ยง

b. กระบวนการในการประเมินความเสี่ยง

c. กระบวนการในการโอนย้ายความเสี่ยง

d. กระบวนการในการยอมรับความเสี่ยง

e. กระบวนการในการลดความเสี่ยงไปสู่ระดับที่ยอมรับได้

26. ข้อใดไม่ใช่ส่วนหนึ่งของการวิเคราะห์ความเสี่ยง (Risk Analysis)

a. การระบุความเสี่ยง

b. จำนวนครั้งของภัยคุกคามที่เกิดขึ้น

c. การจัดความสมดุลระหว่างผลกระทบของความเสี่ยงกับค่าใช้จ่ายในการจัดการความเสี่ยง

d. การเลือกการรับมือความเสี่ยงที่ดีที่สุด

e. ผลกระทบจากภัยคุกคาม

27. ข้อใดไม่ถือว่าเป็นปัจจัยความเสี่ยงที่ปกติของระบบสารสนเทศ

a. คน

b. ธรรมชาติ

c. เทคโนโลยี

d. การเจาะระบบ (Hacking)

e. อายุการใช้งานของอุปกรณ์

32. องค์กรควรทำการทดสอบ Business Continuity Plan บ่อยแค่ไหน

a. ทุก 10 ปี

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

การลงทุนในการป้องกันกรณีนี้ควรมีค่าสูงสุดไม่เกินเท่าไหร่

a. 1,000,000 บาท

b. 400,000 บาท

c. 200,000 บาท

d. 80,000 บาท

e. 40,000 บาท

29. บุคคลใดในองค์กรถือเป็นผู้รับผิดชอบในการบริหารความเสี่ยง (Risk Management)

a. เจ้าของระบบ

b. ผู้ใช้งานระบบ

c. ผู้ดูแลระบบ

d. คณะทำงานบริหารความเสี่ยง

e. ผู้บริหารขององค์กร

30. ในกรณีพบว่าค่าใช้จ่ายในการจัดการความเสี่ยงสูงกว่ามูลค่าความเสี่ยง ควรจะดำเนินการอย่างไร

a. ปฏิเสธความเสี่ยงนั้น

b. หาวิธีการอื่นในการวิเคราะห์ความเสี่ยง

c. ยอมรับความเสี่ยงนั้น
โดยไม่ต้องดำเนินการใดๆ

d. ดำเนินการลดความเสี่ยง

e. ดำเนินการโอนย้ายความเสี่ยง

31. ข้อใดถือเป็นขั้นตอนแรกในการสร้าง Business Continuity Plan

a. กำหนด backup solution

b. การเลือกวิธีการทดสอบ Business Continuity Plan

c. ดำเนินการวิเคราะห์ Business Impact

b. ทุก 1 ปี

c. ทุก 6 เดือน

d. หลังการเปลี่ยนแปลงที่สำคัญของระบบ IT ในองค์กร

e. ถูกทั้งข้อ ข. และ ข้อ ง.

33. วิธีที่สามารถทำให้แน่ใจได้ว่า ข้อมูลที่ทำการ Backup ลงสื่อสำรองต่างๆ สามารถที่จะ restore กลับคืนมาได้อย่างครบถ้วน ณ ศูนย์สำรอง ในกรณีฉุกเฉิน

a. ทำการทดสอบ restore ข้อมูลจากเทปสำรองข้อมูลทั้งที่ศูนย์หลักและที่ศูนย์สำรอง

b. ขอให้ผู้ขายอุปกรณ์ช่วยทดสอบ และทำการติดป้ายเทปที่ผ่านการทดสอบ

c. ทดสอบการอ่านเทปด้วยเครื่องของผู้ขาย ซึ่งไม่ใช่อุปกรณ์จริงที่ใช้ในกรณีฉุกเฉิน

d. เก็บเทปสำรองไว้ที่บริษัทผู้ขายเดือนละ 2 ครั้ง

e. ทำการสำรองข้อมูลลงเทปเป็นประจำทุกวัน

34. ใครเป็นผู้มีอำนาจอนุมัติ Business Continuity Plan ในองค์กร

a. คณะกรรมการวางแผน

b. ตัวแทนจากแผนกต่างๆ

c. ผู้จัดการฝ่าย IT

d. ผู้ตรวจสอบภายนอก

e. คณะผู้บริหารองค์กร

35. ข้อใดคือมาตรฐานสากลที่เกี่ยวกับเรื่อง Business Continuity Management

a. ISO27001

b. BS7799

c. BS25999

d. ISO9001

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

Analysis

d. จัดทำ Business Resumption Plan

e. ดำเนินการวิเคราะห์ Business Recovery Plan

36. ใครต้องเป็นผู้มีส่วนร่วมในการทดสอบ Business Continuity Plan

a. คนที่ต้องการ implement Business Continuity Plan

b. คนที่สนับสนุน หรือองค์กร outsource ที่เกี่ยวข้อง

c. เจ้าของผลิตภัณฑ์ Supplies ที่สำคัญของระบบที่องค์กรใช้งานอยู่

d. ผู้สังเกตการณ์

e. ถูกทุกข้อ

37. ข้อใดให้ความหมายของ Business Continuity Management (BCM) ไม่ถูกต้อง

a. BCM หมายถึงกระบวนในการกู้ระบบ IT ให้กลับมาทำงาน

b. BCM หมายถึงกระบวนการบริหารทางธุรกิจ

c. การรับมือกับเหตุฉุกเฉิน (Incident Response) เป็นส่วนหนึ่งของ BCM

d. BCM ต้องถือเป็นส่วนหนึ่งของวัฒนธรรมองค์กร

e. BCM เพิ่มความสามารถในการดำเนินการขององค์กร

38. เรื่องใดถือว่าสำคัญที่สุดในการทำ Business Continuity Plan

e. ISO20000

40. Recovery Plan ควรจะครอบคลุมส่วนใดขององค์กรบ้าง

a. ฝ่ายปฏิบัติการและฝ่ายการเงินที่สำคัญที่สุด

b. ฝ่ายที่มีความสำคัญยิ่งยวด

c. ทุกฝ่าย

d. ฝ่ายที่หยุดทำงานแล้วทำให้องค์กรไม่สามารถดำเนินธุรกรรมต่อไปได้

e. ฝ่ายที่ผู้บริหารตัดสินว่าสำคัญที่สุด

41. ประเภทของการสแกนที่ใช้ packet with all flags set?

a. Full Open

b. Syn scan

c. TCP connect

d. XMAS scan

e. Null scan

42. คำสั่ง "ln -sf /dev/null /root/.bash_history" ทำอะไร?

a. To rename file bash_history file to null

b. To rename file null to bash_history

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

a. Business Impact Analysis

b. การ Implement การทดสอบ และการติดตามผล

c. การได้รับความร่วมมือจากพนักงานทุกคน จากทุกแผนก

d. การสนับสนุนจากผู้บริหารสูงสุด

e. การได้รับความร่วมมือจากผู้ตรวจสอบ

39. ศูนย์คอมพิวเตอร์สำรอง (Backup Site) มีประเภทอะไรบ้าง

a. Hot Site

b. Warm Site

c. Cold Site

d. ถูกทั้งข้อ ก. และ ข.

e. ถูกทุกข้อ

47. Conflicker/Downadup Worm เราจะต้อง set Firewall ให้ block port อะไร?

a. 445/TCP

b. 111/TCP

c. 1434/UDP

d. 139/UDP

e. 137/TCP

48. ข้อไหนถูกต้องที่สุดที่เกี่ยวกับระบบความมั่นคงทางเครือข่ายแบบไร้สาย

c. To disable the keeping of bash shell command history

d. To link bash shell history to /dev/null

e. To link /dev/null to bash shell history

43. ข้อไหนเป็น passive online attack?

a. SSL spoofing

b. Network sniffing

c. DNS poisoning attack

d. Dictionary attack

e. Man-in-the-Middle attack

44. ข้อไหนเป็นวิธีการดึงข้อมูลโดยที่เหยื่อไม่รู้ตัว

a. Stealth Scan

b. DNS query

c. Traceroute

d. Ping sweep

e. Wardialing

45. ข้อไหนที่เป็นการป้องกันการโจมตีแบบ buffer overflow?

a. Encryption

b. Web Forms

c. Firewall

d. Input field length validation

e. SQL Stored Procedure

46. คำสั่ง SQL ไหนที่ใช้ในการดึงข้อมูล

a. SELECT

b. GET

a. WEP 128-bit มีความยากต่อการ hack เป็น 2 เท่าของ WEP 64-bit

b. WEP 128-bit ต้องใช้ user authentication เท่านั้น

c. WPA PSK สามารถถูก hack ได้โดยวิธี brute force

d. WPA2 มีความเข้มแข็งเป็น 1024 เท่าของ WPA

e. ผู้ใช้ของ WPA2 จะไม่สามารถถูก hack โดยวิธี ARP spoofing

49. ข้อไหนถูกต้องที่สุดที่เกี่ยวกับระบบความมั่นคงทางเครือข่ายแบบมีสาย

a. อุปกรณ์สวิทช์ในระดับ layer 2 ไม่สามารถถูก sniff ได้

b. อุปกรณ์สวิทช์ในระดับ layer 3 มีความปลอดภัยกว่า อุปกรณ์สวิทช์ในระดับ layer 2

c. VLAN สามารถป้องกันการโจมตีแบบ local flooding ได้

d. การโจมตีแบบ ARP flooding ไม่สามารถข้ามไปที่อุปกรณ์สวิทช์ตัวอื่นได้

e. การโจมตีแบบ ARP flooding ไม่สามารถข้ามไปที่อุปกรณ์สวิทช์ในระดับ layer 3 ได้

50. โปรโตคอลใดที่มีความปลอดภัยมากที่สุดจากการโจมตีแบบ sniff?

a. SSH

b. SSL

c. FTP

d. DNS

e. IRC

c. INSERT

d. SET

e. SHOW

51. ประเทศไทยได้ประกาศใช้กฎหมายที่เกี่ยวข้องกับการกระทำความผิดทางคอมพิวเตอร์ แล้ว กี่ฉบับ

a. 1 ฉบับ

b. 2 ฉบับ

c. 3 ฉบับ

d. 4 ฉบับ

e. ไม่มีข้อใดถูกต้อง

52. ความหมายของคำว่า “ข้อมูลจราจรทางคอมพิวเตอร์” ตามพรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 คือ
“ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึง …….
หรืออื่นๆที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น”

a. ต้นทางหรือแหล่งกำเนิด ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ

b. เส้นทาง ต้นทาง ปลายทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ

c. ต้นทาง ปลายทาง วันที่ เวลา ปริมาณ ระยะเวลา ชนิดของบริการ รวมทั้งแหล่งกำเนิด

d. วันที่ เวลา เส้นทางจากต้นทาง ปลายทาง ปริมาณ ระยะเวลา รวมทั้งชนิดของบริการ

e. ไม่มีข้อใดถูกต้อง

53. ความหมายของคำว่า “ผู้ให้บริการ” ตามพรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 คือ

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

54. ตามประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง
หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550
กำหนดให้ผู้ให้บริการต้องตั้งนาฬิกาของอุปกรณ์บริการทุกชนิดให้มีความผิดพลาดไม่เกิน เท่าไหร่

a. 3 มิลลิวินาที

b. 5 มิลลิวินาที

c. 7 มิลลิวินาที

d. 9 มิลลิวินาที

e. ไม่มีข้อใดถูกต้อง

55. ตามประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง
หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550 จำแนกผู้ให้บริการไว้กี่ ประเภท

a. 1 ประเภท

b. 2 ประเภท

c. 3 ประเภท

d. 4 ประเภท

e. ไม่มีข้อใดถูกต้อง

56. ในระบบเครือข่ายส่วนตัวเสมือน (Virtual Private Network หรือ VPN) ผู้ใช้ A
ที่อยู่นอกสถานที่สามารถล็อกออนเข้ามาใช้งานระบบเครือข่ายส่วนตัวภายในหน่วยงานผ่านอินเทอร์เน็ตได้อย่างปลอดภัย คำถามคือ ถ้าในขณะที่ผู้ใช้ A
ล็อกออนอยู่ในระบบเครือข่ายนั้น ผู้ใช้ B
ที่ทำงานอยู่ในตัวอาคารของหน่วยงานด้วยในขณะเดียวกัน จะมองเห็น IP address ของผู้ใช้ A ว่ามาจากไหน

a. เป็น IP address อื่นจากอินเทอร์เน็ต
ขึ้นอยู่กับผู้ให้บริการอินเทอร์เน็ตที่ผู้ใช้ A ใช้อยู่

b. เป็น IP address ในกลุ่มเดียวกันกับระบบ

a. ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต
หรือให้สามารถติดต่อถึงกันโดยประการอื่น
โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้
ไม่ว่าจะเป็นการให้บริการในนามของตนเอง
หรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น

b. ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

c. ผู้ให้บริการแก่บุคคลอื่นๆในการเข้าสู่อินเทอร์เน็ต
หรือให้สามารถติดต่อถึงกันได้โดยผ่านทางระบบคอมพิวเตอร์หรือระบบอื่นๆ ทั้งนี้
ไม่ว่าจะเป็นการให้บริการในนามของตนเอง
หรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น

d. ถูกเฉพาะข้อ a. และ b.

e. ถูกเฉพาะข้อ b. และ c.

57. บัตรเครดิต
มีระบบการเข้ารหัสข้อมูลภายในบัตรด้วยเพื่อป้องกันความลับของข้อมูลภายในบัตรรั่วไหล คุณคิดว่า
การเข้ารหัสที่เหมาะสมกับการใช้งานในบัตรประเภทนี้ควรเป็นการเข้ารหัสชนิดใด

a. Public key

b. Secret key

c. Hash key

d. Master key

e. ไม่มีข้อใดถูกต้อง

58. ร้านค้าสะดวกซื้อ
แห่งหนึ่งตรวจพบว่ามีคนขโมยสินค้า
ทั้งที่สินค้าทุกตัวที่มีการติดตั้งอุปกรณ์ RFID
แต่กลับไม่มีการส่งสัญญาณเตือนภัยเลย อีกทั้งอุปกรณ์ RFID ก็ทำงานได้ดีตามปรกติโดยไม่มีการผิดพลาด
ให้สมมุติว่าคุณเป็นเจ้าหน้าที่ตำรวจที่มาตรวจสอบคดีนี้
คุณจะตั้งสมมุติฐานว่าผู้ขโมยสินค้านั้นสามารถรอดพ้นจากการตรวจเช็กของเครื่องตรวจสัญญาณ RFID ได้อย่างไร

a. พนักงานภายในร้าน เป็นผู้ขโมยเอง

b. ผู้ออกแบบระบบ RFID
ตั้งใจผลิตระบบให้มีช่องโหว่

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

เครือข่ายส่วนตัวของหน่วยงานนั้นเลย

c. เป็น IP address
ที่ถูกเลือกให้โดยหน่วยงานของรัฐบาลที่มีหน้าที่จัดสรรหมายเลข IP ของ VPN โดยเฉพาะ

d. เป็น IP address ของอุปกรณ์ VPN

e. ไม่มีข้อใดถูกต้อง

60. เมื่อคุณพิจารณาแล้วว่า
มีโอกาสที่เครื่องของคุณในร้านจะติดไวรัสได้
คุณจึงวางแผนในการรับมือในกรณีที่เครื่องติดไวรัสที่เหมาะสมที่สุดคือ

a. จัดทำซีดีสะอาดปราศจากไวรัสไว้หนึ่งแผ่นพร้อมทั้งก็อปปี้โปรแกรมฆ่าไวรัสไว้ในแผ่น
เมื่อมีเครื่องใดติดไวรัส ก็ให้ปิดเครื่องนั้น
บูตเครื่องใหม่ด้วยซีดีสะอาด
แล้วจัดการไวรัสด้วยโปรแกรม

b. ปิดเครื่องที่ติดไวรัสไม่ให้ทำงาน
เพื่อป้องกันไม่ให้ไวรัสโจมตีไปยังเครื่องอื่นๆ ของคุณ

c. ฟอร์แมตเครื่องนั้นใหม่ โดยใช้ OS ที่สะอาด
และลงโปรแกรมฆ่าไวรัส

d. นำโปรแกรมฆ่าไวรัส มาใช้ฆ่าไวรัสในเครื่องนั้นๆให้สะอาดก่อน
แล้วจึงนำเครื่องนั้นมาให้ลูกค้าใช้บริการ

e. ไม่มีข้อใดถูกต้อง

61. เป้าหมายหลักของการโจมตีด้วยวิธีการ Port Scan คืออะไร?

a. ค้นหาจุดโหว่ที่เป็นไปได้

b. ระบุ services ที่เปิดให้บริการ

เพื่อให้บุคลากรของบริษัทฯสามารถใช้ช่องโหว่นั้นหาทางเอาสินค้าออกไปได้

c. ผู้ขโมยใส่สินค้าไว้ในภาชนะที่มีวัสดุที่มีคุณสมบัติกันสัญญาณ

d. ผู้ขโมยอาจยกสินค้าไว้เหนือหัวให้สูงกว่าอุปกรณ์ตรวจสัญญาณ RFID

e. ไม่มีข้อใดถูกต้อง

ข้อมูลนี้ใช้สำหรับตอบคำถามข้อ 59-60

คุณได้ลงทุนเปิดกิจการร้าน Internet Cafe
เพื่อให้บริการอินเตอร์เน็ตแก่บุคคลทั่วไป
คุณตัดสินใจที่จะเข้ามาดูแลระบบความมั่นคงปลอดภัยของร้านคุณเอง

59. คุณคิดว่านโยบายป้องกันไวรัสที่เหมาะสมที่สุดสำหรับร้านคุณ เพื่อป้องกันไม่ให้ร้านคุณติดไวรัสคือ

a. ติดตั้ง Antivirus บน Server ของคุณ

b. ไม่อนุญาตให้ลูกค้านำอุปกรณ์ใดๆ มาเสียบเข้าเครื่องของคุณ

c. ออกโทษปรับลูกค้าที่นำไวรัสมาแพร่ในร้านของคุณ

d. ระบบจะไม่เก็บรักษาไฟล์ใดๆ ของลูกค้าไว้หลังจากลูกค้า log off แล้ว

e. ไม่มีข้อใดถูกต้อง

63. What occurs during a spoofing attack?

a. One device falsifies data to gain access to privileged information.

b. Large amounts of network traffic are sent to a target device to make resources unavailable to intended users.

c. Improperly formatted packets are forwarded to a target device to cause the target system to crash.

c. ระบุ operating system

d. ถูกทุกข้อ

e. ไม่มีข้อใดถูกต้อง

62. อะไรเป็นคุณสมบัติของไวรัส

a. ไวรัสต้องมีบุคคลเข้ามามีส่วนร่วมในการทำงาน

b. ไวรัสสามารถหยุดทำงานชั่วคราวแล้วเริ่มต้นทำงานใหม่ในช่วงวันและเวลาที่กำหนด

c. ไวรัสสามารถให้ข้อมูลที่สำคัญ เช่น รหัสผ่านแก่ผู้โจมตี

d. ถูกเฉพาะข้อ a และ b

e. ถูกทุกข้อ

66. What occurs during the persist phase of a worm attack?

a. Identification of vulnerable targets

b. Modification of system files and registry settings to ensure that the attack code is running

d. A program writes data beyond the allocated memory to enable the execution of malicious code.

e. None of the above

64. What is a ping sweep?

a. A ping sweep is a network scanning technique that indicates the live hosts in a range of IP addresses.

b. A ping sweep is a software application that enables the capture of all network packets sent across a LAN.

c. A ping sweep is a scanning technique that examines a range of TCP or UDP port numbers on a host to detect listening services.

d. A ping sweep is a query and response protocol that identifies information about a domain, including the addresses assigned to that domain.

e.None of the above

65. What is a characteristic of a Trojan horse?

a. A Trojan horse can be carried in a virus or worm.

b. A proxy Trojan horse opens port 21 on the target system.

c. An FTP Trojan Horse stops anti-virus programs or firewalls from functioning.

c. Transfer of exploit code through an attack vector

d. Extension of the attack to vulnerable neighboring targets

e. None of the above

67. Which characteristic best describes the network security Compliance domain as specified by the ISO/IEC?

a. The integration of security into applications

b. An inventory and classification scheme for information assets

c. The restriction of access rights to networks, systems, applications, functions, and data

d. The process of ensuring conformance with security information policies, standards, and regulations

e. None of the above

68. Which phase of worm mitigation involves terminating the worm process, removing modified files or system settings that the worm introduced, and patching the vulnerability that the worm used to exploit the system?

a. Containment

b. Inoculation

c. Quarantine

d. Treatment

d. A Trojan horse can be hard to detect because it closes when the application that launched it closes.

e. None of the above

70. Which statement describes access attacks?

a. Port scanning attacks scan a range of TCP or UDP port numbers on a host to detect listening services.

b. Password attacks can be implemented using brute-force attack methods, Trojan Horses, or packet sniffers.

c. Buffer overflow attacks write data beyond the allocated buffer memory to overwrite valid data or exploit systems to execute malicious code.

d. Only b. and c.

e.None of the above

71. Which technology is an example of a host-based intrusion prevention system?

a. DCN

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

e.None of the above

69. A disgruntled employee is using Wireshark to discover administrative Telnet usernames and passwords. What type of network attack does this describe?

a. Denial of Service

b. Port redirection

c. Reconnaissance

d. Trust exploitation

e. None of the above

74. What are the three major components of a worm attack?

a. Enabling vulnerability, Infecting vulnerability, Payload

b. Enabling vulnerability, Payload, Propagation mechanism

c. Propagation mechanism, Penetration mechanism, Probing mechanism

d. Infecting vulnerability, Penetration mechanism, Probing mechanism

e. None of the above

b. NAC

c. CSA

d. VPN

e. None of the above

72. Which phase of worm mitigation requires compartmentalization and segmentation of the network to slow down or stop the worm and prevent currently infected hosts from targeting and infecting other systems?

a. Containment phase

b. Inoculation phase

c. Quarantine phase

d. Treatment phase

e. None of the above

73. Which statement describes phone freaking?

a. A hacker uses password-cracking programs to gain access to a computer via a dialup account.

b. A hacker gains unauthorized access to networks via wireless access points.

c. A hacker mimics a tone using a whistle to make free long-distance calls on an analog telephone network.

d. A hacker uses a program that automatically scans telephone numbers within a local area, dialing each one in search of computers, bulletin board systems, and fax machines.

ตอนที่ 1 โปรดเลือกตัวเลือกที่ถูกต้องที่สุดเพียงตัวเลือกเดียว (ข้อละ 1 คะแนน)

75. Which type of software typically uses a network adapter card in promiscuous mode to capture all network packets that are sent across a LAN?

a. Port scanner

b. Ping sweeper

c. Packet sniffer

d. Internet information query

e. None of the above

76. Which two are characteristics of DoS attacks?

a. 1) They always precede access attacks.

2) They are difficult to conduct and are initiated only by very skilled attackers.

b. 1) They attempt to compromise the availability of a network, host, or application.

2) Examples include smurf attacks and ping of death attacks.

c. 1) They are difficult to conduct and are initiated only by very skilled attackers.

2) They are commonly launched with a tool called L0phtCrack.

d. 1) They are commonly launched with a tool called L0phtCrack.

2) They attempt to compromise the availability of a network, host, or application.

e. 1) Examples include smurf attacks and ping of death attacks.

e. None of the above

77. What are three types of access attacks?

a. Buffer overflow, Port redirection, Trust exploitation

b. Ping sweep, Port scan, Internet information query

c. Port redirection, Port scan, Buffer overflow

d. Ping sweep, Trust exploitation, Internet information query

e. None of the above

78. Which type of security threat can be described as software that attaches to another program to execute a specific unwanted function?

a. Virus

b. Worm

c. Proxy Trojan horse

d. Denial of Service Trojan horse

e. None of the above

79. How is a Smurf attack conducted?

a. By sending a large number of packets, overflowing the allocated buffer memory of the target device

b. By sending an echo request in an IP packet larger than the maximum packet size of 65,535 bytes

2) They always precede access attacks.

81. How do modern cryptographers defend against brute-force attacks?

a. Use statistical analysis to eliminate the most common encryption keys.

b. Use an algorithm that requires the attacker to have both ciphertext and plaintext to conduct a successful attack.

c. Use a key space large enough that it takes too much money and too much time to conduct a successful attack.

d. Use frequency analysis to ensure that the most popular letters used in the language are not used in the cipher message.

e. None of the above.

82. Which two encryption algorithms are commonly used to encrypt the contents of a message?

a. 3DES, IPSec

b. AES, 3DES

c. PKI, IPSec

d. SHA1, AES

e. PKI, SHA1

c. By sending a large number of ICMP requests to directed broadcast addresses from a spoofed source address on the same network

d. By sending a large number of TCP SYN packets to a target device from a spoofed source address

e. None of the above

80. An attacker is using a laptop as a rogue access point to capture all network traffic from a targeted user. Which type of attack is this?

a. Trust exploitation

b. Buffer overflow

c. Man in the middle

d. Port redirection

e. None of the above

85. Which statement describes a cryptographic hash function?

a. A one-way cryptographic hash function is hard to invert.

b. The output of a cryptographic hash function can be any length.

c. The input of a cryptographic hash function has a fixed length.

ตอนที่ 1 โปรดเลือกตัวเลือกที่ถูกต้องที่สุดเพียงตัวเลือกเดียว (ข้อละ 1 คะแนน)

83. Which encryption protocol provides network layer confidentiality?

a. IPSec protocol suite

b. Message Digest 5

c. Secure Sockets Layer

d. Secure Hash Algorithm 1

e. Transport Layer Security

84. What does it mean when a hashing algorithm is collision resistant?

a. Exclusive ORs are performed on input data and produce a digest.

b. It is not feasible to compute the hash given the input data.

c. It uses a two-way function that computes a the input and output data.

d. Two messages with the same hash are unlikely to occur.

e. None of the above

89. Which statement is a feature of HMAC?

a. HMAC is based on the RSA hash function.

b. HMAC uses a secret key that is only known to the sender and defeats man-in- the-middle attacks.

c. HMAC uses a secret key as input to the hash

d. A cryptographic hash function is used to provide confidentiality.

e. None of the above

86. Which symmetrical encryption algorithm is the most difficult to crack?

a. 3DES

b. AES

c. DES

d. RSA

e. SHA

87. Which three primary functions are required to secure communication across network links?

a. Accounting, Authentication, Authorization

b. Anti-replay protection, Confidentiality, Accounting

c. Authentication, Confidentiality, Integrity

d. Integrity, Confidentiality, Authorization

e. None of the above

88. Two users must authenticate each other using digital certificates and a CA. Which option describes the CA authentication procedure?

a. The CA is always required, even after user verification is complete.

b. The users must obtain the certificate of the CA and then their own certificate.

function, adding authentication to integrity assurance.

d. HMAC uses protocols such as SSL or TLS to provide session layer confidentiality.

e. None of the above.

90. Refer to the exhibit. Which encryption algorithm is described in the exhibit?

Timeline	Standardized 1977
Type of Algorithm	Symmetric
Key size (in bits)	112 and 168 bits
Speed	Low
Time to crack (Assuming a computer could try 255 keys per second)	4.6 Billion years with current technology
Resource Consumption	Medium

a. 3DES

b. AES

c. DES

d. RC4

e. SEAL

91. The network administrator for an e-commerce website requires a service that prevents customers

c. After user verification is complete, the CA is no longer required, even if one of the involved certificates expires.

d. CA certificates are retrieved out-of-band using the PSTN, and the authentication is done in-band over a network.

e. None of the above

92. An administrator requires a PKI that supports a longer lifetime for keys used for digital signing operations than for keys used for encrypting data. Which feature should the PKI support?

a. Certificate keys

b. no repudiation keys

c. Usage keys

d. Variable keys

e. None of the above

93. Why RSA is typically used to protect only small amounts of data?

a. The keys must be a fixed length.

b. The public keys must be kept secret.

c. The algorithms used to encrypt data are slow.

d. The signature keys must be changed frequently.

e. None of the above

94. What is the basic method used by 3DES to

from claiming that legitimate orders are fake. What service provides this type of guarantee?

a. Authentication

b. Confidentiality

c. Integrity

d. non repudiation

e. None of the above

96. A customer purchases an item from an e-commerce site. The e-commerce site must maintain proof that the data exchange took place between the site and the customer. Which feature of digital signatures is required?

a. Authenticity of digitally signed data

b. Integrity of digitally signed data

c. Non repudiation of the transaction

d. Confidentiality of the public key

e. None of the above

97. Which two statements correctly describe certificate classes used in the PKI?

a. 1) A class 0 certificate is for testing purposes.

2) A class 0 certificate is more trusted than a class 1 certificate.

b. 1) A class 0 certificate is more trusted than a class 1 certificate.

encrypt plaintext?

a. The data is encrypted three times with three different keys.

b. The data is encrypted, decrypted, and encrypted using three different keys.

c. The data is divided into three blocks of equal length for encryption.

d. The data is encrypted using a key length that is three times longer than the key used for DES.

e. None of the above.

95. What is a characteristic of the RSA algorithm?

a. RSA is much faster than DES.

b. RSA is a common symmetric algorithm.

c. RSA is used to protect corporate data in high-throughput, low-latency environments.

d. RSA keys of 512 bits can be used for faster processing, while keys of 2048 bits can be used for increased security.

e. None of the above.

99. Which statement describes the use of keys for encryption?

a. The sender and receiver must use the same key when using symmetric encryption.

b. The sender and receiver must use the same key when using asymmetric encryption.

2) The lower the class number, the more trusted the certificate.

c. 1) The lower the class number, the more trusted the certificate.

2) A class 5 certificate is for users with a focus on verification of email.

d. 1) A class 5 certificate is for users with a focus on verification of email.

2) A class 4 certificate is for online business transactions between companies.

e. 1) A class 4 certificate is for online business transactions between companies.

2) A class 0 certificate is for testing purposes.

98. Which statement describes asymmetric encryption algorithms?

a. They include DES, 3DES, and AES.

b. They have key lengths ranging from 80 to 256 bits.

c. They are also called shared-secret key algorithms.

d. They are relatively slow because they are based on difficult computational algorithms.

e. None of the above.

c. The sender and receiver must use the same keys for both symmetric and asymmetric encryption.

d. The sender and receiver must use two keys: one for symmetric encryption and another for asymmetric encryption.

e. None of the above.

100. Refer to the exhibit. Which type of cipher method is depicted?

a. Caesar cipher

b. Stream cipher

c. Substitution cipher

d. Transposition cipher

e. None of the above