เอกสารข้อสอบฉบับนี้
จัดทำเพื่อใช้ในการทดสอบในโครงการ
Network Security Contest 2008
ชุดที่ 1 ข้อสอบข้อที่ 1-100

1. **เวลาในการสอบ 3 ชั่วโมง**
2. **การสอบเป็นแบบ ปิดตำรา**
3. **ห้ามนำเอกสารใดๆ เข้าห้องสอบ**
4. **ห้ามใช้เครื่องมือสื่อสารใดๆ ทุกชนิด**
5. **ห้ามนำเอกสารฉบับนี้ออกนอกห้องสอบโดยเด็ดขาด**
6. **ให้ส่งเอกสารฉบับนี้คืนพร้อมกับกระดาษคำตอบ**
7. **การคิดคะแนนทีมที่แข่งขัน จะนำคะแนนของทั้ง 3 คนในทีมมารวมกันเป็นคะแนนของทีม**
8. **การคัดเลือกจะคัดเลือกทีมเข้ารอบสุดท้าย 10 ทีม**
9. **สำหรับทีมที่มาจากมหาวิทยาลัยเดียวกัน จะคัดเลือกทีมที่มีคะแนนสูงสุด 3 ทีมเท่านั้นในการเข้ารอบสุดท้าย**

(คณะกรรมการจัดการแข่งขัน จัดให้มีคณะกรรมการผู้ทรงคุณวุฒิเป็นคณะกรรมการตัดสินการแข่งขัน และผลการตัดสินของคณะกรรมการถือเป็นที่สุด
และคณะผู้จัดทำขอสงวนสิทธิรางวัลชนะเลิศสำหรับทีมที่เหมาะสมที่สุดเท่านั้น)

ห้ามทุจริตในการสอบ
มิฉะนั้นจะถูกตัดสิทธิในการแข่งขันทันที

ชื่อ-นามสกุล .....
ชื่อทีม..... .....
ชื่อสถาบัน
..... **เบอร์ติดต่อ**....
.....

คำถามข้อ 1-10
นาย ก. พึ่งจะได้เรียนวิชา computer security มา
ด้วยความสนุกจึงได้ตัดสินใจลองบุกรุกเข้าไปในระบบของมหาวิทยาลัยที่ตนเองเรียนอยู่
โดยได้พยายามหาช่องโหว่ที่มีอยู่ในระบบ พบว่ามีหลายเครื่องที่น่าสนใจ จึงได้เข้าไปในเครื่องคอมพิวเตอร์ A
โดยนาย ก. ดีใจมากที่สามารถเข้าไปได้ง่าย เพราะเข้าไปได้โดยไม่ต้องป้อนชื่อผู้ใช้และรหัสผ่าน
ซึ่งพบว่าเป็นเครื่อง server ที่เก็บข้อมูลทั่วไปของมหาวิทยาลัยของตน หลังจากนั้น
ก็ลองพยายามเข้าเครื่องคอมพิวเตอร์ B ซึ่งนาย ก. ต้องพยายามหาวิธีการบุกรุกเข้าไป จนสามารถทำได้สำเร็จ
ซึ่งพบว่า เครื่องคอมพิวเตอร์ B เป็น server ที่เก็บข้อมูลรายละเอียดของวิชาคอมพิวเตอร์อยู่ นาย ก.
จึงได้เข้าไปค้นดูรายละเอียดใน server B และพบว่าคะแนนสอบของตนเองในวิชานี้ไม่ดี
จึงได้แก้เกรดของตนเองให้ได้ A หลังจากนั้นก็หยุดเล่น ต่อมาเวลาไม่นาน อาจารย์ที่สอนวิชา computer
ได้เรียก นาย ก. เข้าพบ และได้มีการดำเนินการทางกฎหมายกับนาย ก. ในเวลาต่อมา

1. ข้อใดถูกต้องที่สุด
   a. นาย ก. ไม่ผิด เพราะทำไปด้วยความสนุกเท่านั้น
   b. นาย ก. ไม่ผิด เพราะระบบของมหาวิทยาลัยไม่มีความปลอดภัยเพียงพอ
   c. นาย ก. ผิด เพราะได้เข้าไปบุกรุกเครื่อง A
   d. นาย ก. ผิด เพราะได้เข้าไปบุกรุกเครื่อง B
   e. ถูกทั้งข้อ c และ d
2. กฎหมายที่ใช้ดำเนินการกับนาย ก. คือกฎหมายใด
   a. นาย ก. ไม่ผิด จึงไม่ต้องดำเนินการตามกฎหมายใดๆ ได้
   b. พระราชบัญญัติว่าด้วยการบุกรุกระบบคอมพิวเตอร์
   c. พระราชกำหนดว่าด้วยการบุกรุกระบบคอมพิวเตอร์
   d. พระราชกำหนดว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

e. ไม่มีข้อใดถูกต้อง

3. ข้อใดถูกต้องที่สุด
   a. อาจารย์ผิด เพราะใส่ข้อมูลเกรดลงในเครื่อง server
   b. นาย ก. ไม่ทำผิดกฎหมาย
   c. นาย ก. ผิด เพราะนาย ก. บุกรุกเครื่องคอมพิวเตอร์ A
   d. นาย ก. ผิด เพราะนาย ก. แก้ไขข้อมูลบนเครื่องคอมพิวเตอร์ B
   e. ถูกทั้งข้อ c และ d

4. ข้อใดถูกต้องที่สุด
   a. นาย ก. ไม่ผิดกฎหมาย ดังนั้น อาจารย์ไม่สามารถดำเนินการตามกฎหมายกับนาย ก.ได้
   b. นาย ก. ทำผิดตามกฎหมายมาตรา 8
   c. นาย ก. ทำผิดตามกฎหมายมาตรา 9
   d. นาย ก. ทำผิดตามกฎหมายมาตรา 10
   e. ถูกทั้งข้อ b,c และ d

5. โทษสูงสุดที่นาย ก. ได้รับคือ
   a. นาย ก. ไม่ต้องจำคุกใดๆ
   b. นาย ก. จำคุกสูงสุดไม่เกิน 3 ปี
   c. นาย ก. จำคุกสูงสุดไม่เกิน 6 ปี
   d. นาย ก. จำคุกสูงสุดไม่เกิน 9 ปี
   e. นาย ก. จำคุกสูงสุดไม่เกิน 12 ปี

6. โทษต่ำสุดที่นาย ก. ได้รับคือ
   a. นาย ก. ไม่ต้องจำคุกใดๆ
   b. นาย ก. จำคุก แต่สามารถรอลงอาญาไว้ก่อน
   c. นาย ก. จำคุก 6 เดือน
   d. นาย ก. จำคุก 1 ปี
   e. ไม่มีข้อใดถูกต้อง

7. ข้อใดถูกต้องที่สุด
   a. นาย ก. ไม่ผิดที่บุกรุกเครื่อง A
   b. นาย ก. ไม่ผิดที่บุกรุกเครื่อง B
   c. นาย ก. ผิดที่บุกรุกเครื่อง A
   d. นาย ก. ผิดที่บุกรุกเครื่อง B
   e. ไม่มีข้อใดถูกต้อง

8. ข้อใดถูกต้องที่สุด
   a. นาย ก. ไม่ผิด
   b. นาย ก. ทำผิดกฎหมาย 1 มาตรา
   c. นาย ก. ทำผิดกฎหมาย 2 มาตรา
   d. นาย ก. ทำผิดกฎหมาย 3 มาตรา
   e. ไม่มีข้อใดถูกต้อง

9. ข้อใดถูกต้องที่สุด
   a. นาย ก. ไม่ได้ทำผิด เพราะนาย ก. ไม่ได้ฆ่าใคร
   b. นาย ก. ไม่ได้ทำผิด เพราะนาย ก. เล่นสนุก
   c. นาย ก. ไม่ได้ทำผิด เพราะระบบเครือข่ายมหาวิทยาลัยไม่ดี
   d. นาย ก. ไม่ได้ทำผิด เพราะนาย ก. ใช้ความรู้ที่เรียนมาทดสอบ
   e. ไม่มีข้อใดถูกต้อง

10. ข้อใดถูกต้องที่สุด
   a. นาย ก. ทำผิด เพราะนาย ก. บุกรุกเครื่อง A
   b.นาย ก. ทำผิด เพราะนาย ก. บุกรุกเครื่อง B
   c. นายก. ทำผิด เพราะนาย ก. แก้ไขข้อมูลเครื่อง B
   d.ถูกทั้งข้อ a. b. และ c.
   e.ไม่มีข้อใดถูกต้อง

คำถามข้อ 11-15

นส. ข. มีความสนุกคึกคะนอง ใช้เวลาว่างในการอ่าน email เล่น chat เพื่อให้บริการแก่เพื่อนๆ ในอินเตอร์เน็ตเพื่อที่จะได้ทำความรู้จักกัน ต่อมา นส. ข. ได้รับ email ที่มีรูปภาพตัดต่อของดาราชื่อดัง ก็รู้สึกตื่นเต้น จึงได้ทำการ forward email ดังกล่าวในกลุ่มเพื่อน รวมทั้งนำไป post ใน web board ต่างๆ

11. นส. ข. ทำผิดกฎหมายหรือไม่
   a. นส. ข. ไม่ได้ทำผิดกฎหมายใดๆ
   b. นส. ข. ทำผิดกฎหมายมาตรา 14
   c. นส. ข. ทำผิดกฎหมายมาตรา 15
   d. นส. ข. ทำผิดกฎหมายมาตรา 16
   e. ไม่มีข้อใดถูกต้อง

12. นส. ข. ทำผิดกี่มาตรา
   a. นส. ข. ไม่ได้ทำผิดกฎหมายใดๆ
   b. นส. ข. ทำผิด 1 มาตรา

c. นส. ข. ทำผิด 2 มาตรา d. นส. ข. ทำผิด 3 มาตรา
e. ไม่มีข้อใดถูกต้อง

13. นส. ข. ได้รับโทษสูงสุดคืออะไร
a. นส. ข. ไม่ได้ทำผิดกฎหมายใดๆ b. นส. ข. รับโทษจำคุกสูงสุดไม่เกิน 1 ปี
c. นส. ข. รับโทษจำคุกสูงสุดไม่เกิน 3 ปี d. นส. ข. รับโทษจำคุกสูงสุดไม่เกิน 5 ปี
e. ไม่มีข้อใดถูกต้อง

14. ข้อใดถูกต้องที่สุด
a. นส. ข. ไม่ได้ทำผิดกฎหมายใดๆ b. นส. ข. ทำผิดในการ forward email ในกลุ่มเพื่อน
c. นส. ข. ทำผิดในการ post ใน web board ต่างๆ d.ถูกทั้งข้อ b. และ c.
e. ไม่มีข้อใดถูกต้อง

15. ผู้ใดจะถูกดำเนินการตามกฎหมาย
a. ไม่มีผู้ใดถูกดำเนินการตามกฎหมาย
b. เพื่อนคนที่ส่งให้ นส. ข.
c. เพื่อนคนที่ส่งให้ นส. ข. และ นส. ข.
d. เพื่อนคนที่ส่งให้ นส. ข และ นส.ข รวมทั้ง เพื่อนที่ นส.ข. ส่ง email ไปให้
e. เพื่อนคนที่ส่งให้ นส. ข และ นส.ข รวมทั้ง เพื่อนที่ นส.ข. ส่ง email ไปให้ และเจ้าของ web board

คำถามข้อ 16-20

นาย ค. ได้จบการศึกษาทางด้านคอมพิวเตอร์มาหมาดๆ ก็มีความรู้ ร้อนวิชา จึงได้เปิดร้านอินเตอร์เน็ต ต่อมาเวลาไม่นาน ได้มีเจ้าหน้าที่ตำรวจเข้ามาที่ร้าน และขอยึดเครื่องคอมพิวเตอร์ทั้งหมด โดยอ้างว่าทางร้านอินเตอร์เน็ตได้ทำผิดกฎหมายที่มีผู้กระทำผิดได้เข้ามาใช้เครื่องที่ร้านของนาย ค. เข้าไปทำผิด โดยที่นาย ค. เองก็ไม่ทราบว่าเป็นใครที่เข้ามาใช้บริการในร้านของตน

16. นาย ค. ทำผิดกฎหมายหรือไม่
a. นาย ค. ไม่ได้ทำผิดกฎหมายใดๆ b. นาย ค. ทำผิดกฎหมายมาตรา 14
c. นาย ค. ทำผิดกฎหมายมาตรา 15 d. นาย ค. ทำผิดกฎหมายมาตรา 16
e. ไม่มีข้อใดถูกต้อง

17. นาย ค. ทำผิดกี่มาตรา
a. นาย ค. ไม่ได้ทำผิดกฎหมายใดๆ b. นาย ค. ทำผิด 1 มาตรา
c. นาย ค. ทำผิด 2 มาตรา d. นาย ค. ทำผิด 3 มาตรา
e. ไม่มีข้อใดถูกต้อง

18. นาย ค. ได้รับโทษสูงสุดคืออะไร
a. นาย ค. ไม่ได้ทำผิดกฎหมายใดๆ b. นาย ค. รับโทษจำคุกสูงสุดไม่เกิน 1 ปี
c. นาย ค. รับโทษจำคุกสูงสุดไม่เกิน 3 ปี d. นาย ค. รับโทษจำคุกสูงสุดไม่เกิน 5 ปี
e. ไม่มีข้อใดถูกต้อง

19. ข้อใดถูกต้องที่สุด
a. นาย ค. ไม่ได้ทำผิดกฎหมายใดๆ b. นาย ค. ทำผิดในการเปิดร้านอินเตอร์เน็ต
c. นาย ค. ทำผิดในการเปิดร้านอินเตอร์เน็ตโดยให้ผู้กระทำผิดเข้ามาใช้เครื่องของนาย ค.
d. ถูกทั้งข้อ b. และ c. e. ไม่มีข้อใดถูกต้อง

20. ข้อใดถูกต้องที่สุด
a. นาย ค. ไม่ได้ทำผิดและเจ้าหน้าที่ตำรวจก็ไม่ได้ทำผิด b.นาย ค. ไม่ได้ทำผิด แต่เจ้าหน้าที่ตำรวจทำผิด
c. นาย ค. ทำผิด โดยที่เจ้าหน้าที่ตำรวจทำได้ถูกต้อง d.นาย ค. ทำผิด และเจ้าหน้าที่ตำรวจก็ทำผิดด้วย
e. ไม่มีข้อใดถูกต้อง

คำถามข้อ 21-30

ท่านเป็นที่ปรึกษาทางด้านกฎหมายที่เกี่ยวข้องกับคอมพิวเตอร์ และได้ให้ความรู้ทางด้านนี้ให้กับองค์กรต่างๆ ท่านจะต้องตอบคำถามดังต่อไปนี้ให้ถูกต้อง

21. กฎหมายที่ระบุถึงความผิดของการทำผิดทางด้านระบบคอมพิวเตอร์
a. มีอยู่ 1 ฉบับ b. มีอยู่ 2 ฉบับ c. มีอยู่ 3 ฉบับ d. มีอยู่ 4 ฉบับ e.ไม่มีข้อใดถูกต้อง

22. กฎหมายในข้อ 21 จะมีกฎหมายหนึ่งฉบับที่ระบุอย่างชัดเจนเกี่ยวกับการทำผิดทางด้านระบบคอมพิวเตอร์ ซึ่งหน่วยงานในแต่ละองค์กรต้องดำเนินการตามกฎหมายฉบับนั้นในมาตราใด
a. มาตรา 27 b.มาตรา 28 c.มาตรา 29 d.มาตรา 30 e.ไม่มีข้อใดถูกต้อง

23. จากกฎหมายในข้อ 22 มีทั้งสิ้นกี่มาตรา
a. 30 มาตรา b. 31 มาตรา c. 32 มาตรา d. 33 มาตรา e.ไม่มีข้อใดถูกต้อง

24. จากกฎหมายในข้อ 22 มีทั้งสิ้นกี่หมวด
a. 1 หมวด b. 2 หมวด c. 3 หมวด d. 4 หมวด e.ไม่มีข้อใดถูกต้อง

25. จากกฎหมายในข้อ 22 มีมาตราใดที่มีโทษสำหรับพนักงานเจ้าหน้าที่
a. มาตรา 22 b.มาตรา 23 c.มาตรา 24 d.ถูกทั้งข้อ a. b. และ c. e.ไม่มีข้อใดถูกต้อง

26. จากกฎหมายในข้อ 22 มีมาตราใดที่ระบุว่าข้อมูลคอมพิวเตอร์สามารถใช้เป็นหลักฐานได้
a. ไม่มีระบุไว้ในมาตราใดๆ b.มาตรา 25 c.มาตรา 26
d. ถูกทั้งข้อ b. และ c. e.ไม่มีข้อใดถูกต้อง

27. จากกฎหมายในข้อ 22 มาตราที่มีความผิดสูงสุด จะมีโทษสูงสุดคือ
a. ประหารชีวิต b.จำคุกตลอดชีวิต c.จำคุก 40 ปี d.จำคุก 20 ปี e.ไม่มีข้อใดถูกต้อง

28. จากข้อ 27 มาตราที่มีความผิดสูงสุดคือ มาตราใด
a. มาตรา 10 b.มาตรา 11 c.มาตรา 12 d.มาตรา 13 e.ไม่มีข้อใดถูกต้อง

29. จากกฎหมายในข้อ 22 มาตราที่มีความผิดต่ำสุด คือมาตราใด
a. มาตรา 10 b.มาตรา 11 c.มาตรา 12 d.มาตรา 13 e.ไม่มีข้อใดถูกต้อง

30. ข้อมูลใดดังต่อไปนี้ ไม่ต้องเก็บไว้ให้พนักงานเจ้าหน้าที่เข้ามาตรวจสอบ
a. ข้อมูล IP Address b.ข้อมูล วัน เวลา c.ข้อมูล Status Indicator
d. ข้อมูล User ID e.ไม่มีข้อใดถูกต้อง

31. ในการกำหนดระดับความสำคัญของทรัพย์สินจะคำนึงถึงสิ่งใดเป็นหลัก
a. ประเภทของผู้เข้าถึงข้อมูล ได้แก่ พนักงาน พนักงานชั่วคราว และลูกค้า
b. Confidentiality, Integrity และ Availability
c. การประเมินระดับความเสี่ยง
d. การประเมินระดับความเสี่ยงและการป้องกันที่ปิดไป
e. การควบคุมการเข้าถึงที่ใช้ในการป้องกันข้อมูล

32. ในการวางแผนและดำเนินการจัดทำขั้นตอนการควบคุมการเข้าถึง (Access Control) ของระบบสารสนเทศ ข้อใดที่ไม่เกี่ยวข้อง
a. ภัยคุกคามที่มีต่อระบบ b.ช่องโหว่ของระบบ
c.ช่องโหว่ของระบบที่เกี่ยวข้องกับไวรัส
d. ความเสี่ยงของภัยคุกคาม e.โอกาสที่เกิดของภัยคุกคาม

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

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

35. ข้อใดหมายถึงจุดอ่อนหรือการขาดการป้องกันการโจมตีของระบบสารสนเทศ
a. ความเสี่ยง b.ภัยคุกคาม c.ช่องโหว่ d.เหตุการณ์ถูกโจมตี
e.ผลกระทบของเหตุการณ์ที่เกิด

36. ข้อใดที่ไม่ถือเป็นวิธีที่ใช้ในการป้องกันหรือลดความเสี่ยงของการละเมิดการเข้าถึงระบบทั้งจากภายในและภายนอก
a. Backup b.Fault tolerance c.Disaster Recovery Planning
d. Business Continuity Planning e.การทำประกัน

37. ข้อใดเป็นสิ่งแรกในการป้องกันด้านความลับ (Confidentiality) ของข้อมูล
a. การติดตั้ง firewall b.การติดตั้งการเข้ารหัส

c. การระบุสารสนเทศที่มีความสำคัญ
d. การพิสูจน์ตัวตนในการเข้าถึงของผู้ใช้งานระบบ
e. การตรวจสอบสิทธิในการเข้าถึงของผู้ใช้งานระบบ

38. ในการพัฒนาระบบสารสนเทศนั้น การวิเคราะห์ความเสี่ยง (Risk Analysis) ควรจะดำเนินการในขั้นตอนใดมากที่สุด
a. Project Initiation b.Requirements definition
c. System Design d.System Construction
e. Implementation Planning

39. ข้อใดอธิบายถึงความหมายของการบริหารความเสี่ยง (Risk Management) ได้ดีที่สุด
a. กระบวนการในการกำจัดความเสี่ยง b.กระบวนการในการประเมินความเสี่ยง
c. กระบวนการในการโอนย้ายความเสี่ยง d.กระบวนการในการยอมรับความเสี่ยง
e กระบวนการในการลดความเสี่ยงไปสู่ระดับที่ยอมรับได้

40. ข้อใดไม่ใช่ส่วนหนึ่งของการวิเคราะห์ความเสี่ยง (Risk Analysis)
a. การระบุความเสี่ยง
b. จำนวนครั้งของภัยคุกคามที่เกิดขึ้น
c. การจัดความสมดุลระหว่างผลกระทบของความเสี่ยงกับค่าใช้จ่ายในการจัดการความเสี่ยง
d. การเลือกการรับมือความเสี่ยงที่ดีที่สุด
e. ผลกระทบจากภัยคุกคาม

41. ความเสี่ยงที่เหลือ (Residual Risk) หมายถึงข้อใด
a. ความเสี่ยงด้านความปลอดภัยที่เหลือก่อนดำเนินการควบคุม
b. ความเสี่ยงด้านความปลอดภัยที่เหลือหลังจากดำเนินการควบคุม
c. จุดอ่อนของทรัพย์สินที่ภัยคุกคามสามารถโจมตีได้
d. ความเสี่ยงที่เหลือหลังจากดำเนินการวิเคราะห์ความเสี่ยง
e. ผลจากเหตุการณ์ที่ไม่พึงประสงค์

42. การรับมือความเสี่ยง (Risk Mitigation) และการควบคุมเพื่อลดความเสี่ยง หมายถึงข้อใด
a. preventive, corrective และ administrative
b.detectiveและ corrective
c. preventive และ detective
d.preventive, detective และ corrective
e. administrative, operation และ corrective

43. ข้อใดไม่ถือว่าเป็นปัจจัยความเสี่ยงที่ปกติของระบบสารสนเทศ
a. คน b.ธรรมชาติ c.เทคโนโลยี d.การเจาะระบบ (Hacking)
e.อายุการใช้งานของอุปกรณ์

44. ความเสี่ยงทุกเรื่องต้องสามารถ
a. โอนย้ายได้ b.กำจัดได้ c.ระบุได้ d.ประกันได้ e.ลดได้

45. ในการพิจารณาหาค่าใช้จ่ายที่ใช้ดำเนินการระบบการควบคุมการเข้าถึงระบบสารสนเทศ สิ่งที่ต้องคำนึงมากที่สุด
a. มูลค่าของข้อมูลหรือทรัพย์สินที่ดำเนินการป้องกัน
b. ความสำคัญของข้อมูลหรือทรัพย์สินในมุมมองของผู้บริหาร
c. งบประมาณของแผนงานกับค่าใช้จ่ายที่เพิ่มขึ้น
d. ค่าใช้จ่ายในการเปลี่ยนข้อมูลที่สูญหาย
e. ค่าใช้จ่ายในการจัดซื้อระบบมาใช้ในครั้งแรก

46. การดำเนินการควบคุมความเสี่ยงมีจุดประสงค์เพื่อที่จะ
a. กำจัดความเสี่ยงและลดความเสียหายที่จะเกิดขึ้น
b. ลดความเสี่ยงและกำจัดความเสียหายที่จะเกิดขึ้น
c. ลดความเสี่ยงและลดความเสียหายที่จะเกิดขึ้น
d. กำจัดความเสี่ยงและกำจัดความเสียหายที่จะเกิดขึ้น
e. ถูกทุกข้อ

47. ในกรณีที่บริษัทต้องการจะทำการป้องกันทรัพย์สินที่มีมูลค่า 1,000,000 บาท จากภัยคุกคามที่มีโอกาสเกิดขึ้น 1 ครั้งในทุก 5 ปี และค่าความเสียหายคิดเป็น 40% ของมูลค่าทรัพย์สิน การลงทุนในการป้องกันกรณีนี้ควรมีค่าสูงสุดไม่เกินเท่าไหร่
a. 1,000,000 บาท b.400,000 บาท c.200,000 บาท

d.80,000 บาท e.40,000 บาท

48. บุคคลใดในองค์กรถือเป็นผู้รับผิดชอบในการบริหารความเสี่ยง (Risk Management)
a. เจ้าของระบบ b.ผู้ใช้งานระบบ c.ผู้ดูแลระบบ
d.คณะทำงานบริหารความเสี่ยง
e. ผู้บริหารขององค์กร

49. สมชายมีหน้าที่รับผิดชอบในการวางแผนการบริหารความเสี่ยง ในส่วนของการจัดลำดับความสำคัญของความเสี่ยงที่ระบุ ถือว่าสมชายทำงานในส่วนใด
a. การประเมินความเสี่ยง b.ความเสี่ยงที่เหลือ c.การควบคุมความปลอดภัย
d. การจัดระดับความสำคัญของทรัพย์สิน e.ถูกทุกข้อ

50. ในด้านความปลอดภัยสารสนเทศ ข้อใดอธิบายถึงส่วนประกอบของความเสี่ยงได้ดีที่สุด
a. ภัยคุกคามและการรั่วไหล b.ภัยคุกคามและช่องโหว่ c.ช่องโหว่และการโจมตี
d. ภัยคุกคามและการโจมตี e.ช่องโหว่และการรั่วไหล

51. ข้อใดเป็นสิ่งแรกในการป้องกันด้านถูกต้องสมบูรณ์ (Integrity) ของข้อมูล
a. การติดตั้ง firewall b.การติดตั้งการเข้ารหัส
c. การระบุสารสนเทศที่มีความสำคัญ
d.การพิสูจน์ตัวตนในการเข้าถึงของผู้ใช้งานระบบ
e. การตรวจสอบสิทธิในการเข้าถึงของผู้ใช้งานระบบ

52. ในปัจจุบัน มีการโจรกรรมข้อมูลสารสนเทศจากกลุ่มใดมากที่สุด
a. แฮกเกอร์ b.หน่วยสืบราชการลับข้ามชาติ
c.ผู้ก่ออาชญากรรมในระหว่างประเทศ
d. พนักงานขององค์กร e.Outsource

53. สิ่งที่ต้องคำนึงถึงเป็นอันดับแรกในการดำเนินการบริหารความเสี่ยงคือ
a. ต้องครอบคลุมความเสี่ยงที่ระบุทั้งหมด b.ต้องคำนึงถึงความคุ้มค่าของค่าใช้จ่าย
c. ต้องตรวจสอบการลงทุนได้
d.ต้องเหมาะสมกับมูลค่าของระบบสารสนเทศ
e. ต้องคำนึงถึงประสิทธิภาพในการจัดการความเสี่ยง

54. ในกรณีพบว่าค่าใช้จ่ายในการจัดการความเสี่ยงสูงกว่ามูลค่าความเสี่ยง ควรจะดำเนินการอย่างไร
a. ปฏิเสธความเสี่ยงนั้น b.หาวิธีการอื่นในการวิเคราะห์ความเสี่ยง
c. ยอมรับความเสี่ยงนั้น d.ดำเนินการลดความเสี่ยง
e. ดำเนินการโอนย้ายความเสี่ยง

55. ในการพัฒนาระบบ การลดความเสี่ยงควรจะดำเนินการในขั้นตอนใดบ้าง
a. ขั้นตอนเริ่มต้นโครงการ b.ขั้นตอนพัฒนาระบบ
c. ขั้นตอนการกำจัดระบบหลังจากเลิกใช้งาน d.ถูกทุกข้อ
e. ถูกทั้ง a. และ b.

56. ข้อใดไม่ใช่บทบาทของผู้บริหารในการจัดการความปลอดภัยสารสนเทศ
a. ให้การสนับสนุน b.ดำเนินการวิเคราะห์ความเสี่ยง
c. กำหนดขอบเขตและความมุ่งหมาย
d.มอบหมายหน้าที่และความรับผิดชอบ
e. ตัดสินใจเลือกการจัดการความเสี่ยง

57. ข้อใดไม่ใช่จุดประสงค์ของการทำการประเมินความเสี่ยง
a. การมอบหมายหน้าที่ความรับผิดชอบ b.การคำนวณหาผลกระทบจากภัยคุกคามที่อาจจะเกิดขึ้น
c. การระบุความเสี่ยง d.การระบุช่องโหว่
e. การหาความสมดุลระหว่างผลกระทบของความเสี่ยงกับค่าใช้จ่ายในการจัดการความเสี่ยง

58. ในการจัดการความเสี่ยง กรณีไหนที่หลังจากประเมินความเสี่ยงแล้ว ไม่ดำเนินการใดๆ เลย ถือว่าเป็นการกระทำที่ยอมรับได้
a. ระบบการเมืองป้องกันความเสี่ยงประเภทนั้นแล้ว
b. วิธีการจัดการความเสี่ยงนั้นซับซ้อนเกินไป
c. วิธีการจัดการความเสี่ยงนั้นไม่ทันสมัย
d. ค่าใช้จ่ายในการจัดการสูงเกินกว่ามูลค่าของความเสียหาย
e. ไม่ข้อใดถูก เพราะว่าความปลอดภัยที่ดีคือการลดผลกระทบของทุกความเสี่ยง

59. ภัยคุกคามส่วนใหญ่เกิดจากอะไร
a. พนักงานที่ไม่พอใจองค์กร
b. ความผิดพลาด และความประมาทของคน
c. ไฟ น้ำ ไฟฟ้า
d. บุคคลภายนอก
e. แฮกเกอร์

60. จุดอ่อนของระบบในการขาดการควบคุมเพื่อป้องกันภัยคุกคามที่มีผลต่อระบบสารสนเทศหรือเครือข่ายถือเป็น

a. ช่องโหว่ b.ความเสี่ยง c.ภัยคุกคาม d.ความประมาท e.Buffer overflow

Virus

61. เมื่อตรวจพบ virus ชื่อ W32/Mydoom.bb@mm ชื่อของ virus ตัวนี้บอกอะไรบ้าง

a. ชื่อของ virus ตัวนี้คือ Mydoom.bb

b. มีความสามารถที่จะส่งตัวเองผ่านทุก e-mail address ที่อยู่ใน mailbox

c. Virus ชนิดนี้โจมตีใน platform ของ windows 32 bit

d. ถูกทั้งข้อ a และ c

e. ถูกทั้งข้อ b และ c

62. ข้อใดคือคุณสมบัติของ virus

a. คัดลอกตัวเองและส่งตัวเองไปยังเครื่องอื่นๆโดยไม่แพร่เชื้อไปติดไฟล์อื่น สร้างความเสียหายให้กับ ระบบเครือข่าย

b. ไม่สามารถส่งตัวเองไปยังเครื่องอื่นๆได้ ไม่แพร่เชื้อไปติดไฟล์อื่น สิ่งที่มันทำคือเปิดโอกาสให้ผู้ไม่ ประสงค์ดีเข้ามาควบคุมเครื่องที่ติดเชื้อจากระยะไกล

c. ไม่สามารถส่งตัวเองไปยังคอมพิวเตอร์เครื่องอื่นๆ แพร่เชื้อไปติดไฟล์อื่นๆในคอมพิวเตอร์โดยการแนบ ตัวมันเองเข้าไป สร้างความเสียหายให้กับไฟล์

d. ไม่สามารถส่งตัวเองไปยังคอมพิวเตอร์เครื่องอื่นๆ ไม่แพร่เชื้อไปติดไฟล์อื่น สิ่งที่มันทำคือรบกวนและละเมิดความเป็นส่วนตัวของผู้ใช้

e. ถูกทั้งข้อ b และ d ขึ้นอยู่กับประเภทของ virus

63. จำเป็นหรือไม่ที่จะต้องปิด System restore ในเครื่องคอมพิวเตอร์ เพื่อป้องกัน virus

a. ไม่จำเป็น เพราะ ถ้าปิด System restore แล้วทำให้ไม่สามารถกู้คืนระบบ windowsเมื่อเกิดความเสียหาย ได้

b. จำเป็น เพราะ virus อาศัยคุณสมบัติการกู้คืนของ System Restore มากู้ virus ที่ถูกฆ่าทิ้งไปแล้วให้คืนกลับมาได้

c. ไม่จำเป็น เพราะ แค่ติดตั้ง anti-virus ก็สามารถป้องกัน virus ได้แล้ว

d. จำเป็น เพราะ เมื่อปิด system restore แล้ว virus จะไม่สามารถเข้าไปแก้ไขค่า registry ในเครื่องคอมพิวเตอร์ได้

e. ไม่จำเป็น เพราะ virus ที่ถูก ฆ่าทิ้งไปแล้วจะถูกลบทิ้งไปจากเครื่อง โดยไม่สามารถจะ Restore กลับมาได้

64. ระบบต่างๆที่อยู่ภายในเครื่องคอมพิวเตอร์ที่เกี่ยวข้องกับการทำงานของ Virus ที่ควรระวังมีอะไรบ้าง

a. Autorun b. hidden file c. system restore d. ถูกทั้ง a และ b e. ถูกทั้ง a , b และ c

65. ข้อใดที่<u>ไม่ใช่</u>อาการที่ควรจะสงสัยว่าเครื่องติดไวรัส

a. ตรวจพบไฟล์นามสกุล **vbs** ทั้งในเครื่องและอุปกรณ์ต่อพ่วง

b. ซีพียูทำงานตลอดเวลา 100% โดยที่เราไม่ได้เปิดหรือใช้งานโปรแกรมอะไรในขณะนั้น

c. ติดหน้าจอ Log in + ต้องใส่ Password ที่เราไม่เคยตั้ง

d. Blue screen of Dead

e. Generic Host Process" error message

Spyware

66. ข้อใดสามารถบ่งชี้ว่าเครื่องคอมพิวเตอร์ติด spyware
   a. มีหน้าต่างเล็กๆ ที่เป็นโฆษณาป๊อบอัพขึ้นมาเมื่อเปิด website
   b. มีแถบเครื่องมือใหม่ๆ ที่ไม่เคยเห็น หรือไม่คุ้นเคยเกิดขึ้นบนเว็บบราวเซอร์และ task tray
   c. มีข้อความแปลกๆตรง title bar ของ Internet explorer
   d. ไม่สามารถ click หรือ double click drive หรือ flash drive ได้
   e. ถูกทุกข้อ

67. ข้อใด<u>ไม่ใช่</u>วิธีการป้องกันไม่ให้ spyware เข้ามายังเครื่องคอมพิวเตอร์
   a. เมื่อมีหน้า popup ขึ้นมาแสดงข้อความ ถามหรือ โฆษณา ให้กดปุ่ม close เท่านั้น ไม่ควรปิด โดยกด X ที่หน้า popup
   b. ปรับแต่งค่าความปลอดภัยบน web browser ให้อยู่ในระดับที่มีความปลอดภัยสูง
   c. อ่าน ข้อความ "Privacy Policy" ให้ละเอียดก่อนที่จะมีการลงโปรแกรมในเครื่อง
   d. .ระวังอีเมล์ ที่แนะนำโปรแกรมฟรีที่ เกี่ยวกับกำจัด spyware
   e. Update windows อย่างสม่ำเสมอ

68. ข้อใดคือการกระทำ ของ spyware
   a. สปายแวร์แก้ไขไฟล์ DLLS (dynamically linked libraries) ของเครื่องคอมพิวเตอร์ที่ใช้งานเพื่อเชื่อมต่อกับอินเทอร์เน็ต
   b. ลบข้อมูลใน registry และขัดขวางการทำงานของ windows
   c. ทำให้เครื่องคอมพิวเตอร์และ web browser ทำงานช้าลง
   d. สามารถส่งตัวเองไปยังเครื่องอื่นๆและแพร่เชื่อไปติดไฟล์อื่นๆได้
   e. ถูกทั้งข้อ a, b และ c

69. spyware มีคุณสมบัติอย่างไร
   a. คัดลอกตัวเองและส่งตัวเองไปยังเครื่องอื่นๆโดยไม่แพร่เชื้อไปติดไฟล์อื่น สร้างความเสียหายให้กับระบบเครือข่าย
   b. ไม่สามารถส่งตัวเองไปยังเครื่องอื่นๆได้ ไม่แพร่เชื้อไปติดไฟล์อื่น สิ่งที่มันทำคือเปิดโอกาสให้ผู้ไม่ประสงค์ดีเข้ามาควบคุมเครื่องที่ติดเชื้อจากระยะไกล
   c. ไม่สามารถส่งตัวเองไปยังคอมพิวเตอร์เครื่องอื่นๆ แพร่เชื้อไปติดไฟล์อื่นๆในคอมพิวเตอร์โดยการแนบตัวมันเองเข้าไป สร้างความเสียหายให้กับไฟล์
   d. ไม่สามารถส่งตัวเองไปยังคอมพิวเตอร์เครื่องอื่นๆ ไม่แพร่เชื้อไปติดไฟล์อื่น สิ่งที่มันทำคือรบกวนและละเมิดความเป็นส่วนตัวของผู้ใช้
   e. คัดลอกตัวเองและส่งตัวเองไปยังเครื่องอื่นๆ และแพร่เชื้อไปติดไฟล์อื่น ทำลายไฟล์

70.ข้อใด<u>ไม่ใช่</u>เครื่องมือที่ใช้กำจัด spyware
   a. Spybot Search & Destroy
   b. Ad-ware
   c. Navarre Webroot Spy Sweeper
   d. Counter Spy
   e. Electronic pox

Spam

71. ข้อใดที่<u>ไม่ใช่</u>เทคนิคที่มีจุดมุ่งหมายเพื่อใช้ทำ spam mail
   a. ใช้ Spider (Robot Engine) เพื่อรวบรวม E-mail จาก Search Engine หรือ Webboard
   b. ใช้ Spy Wareในการรวบรวมข้อมูลพฤติกรรมการใช้งาน Internet ของ user
   c. ใช้เทคนิค pharming ในการล่อลวง user
   d. virus ที่อยู่ในเครื่องของ User เป็นตัวสร้าง Spam mail ส่งออกไปยังปลายทาง
   e. hacker เจาะเข้าสู้ server ต่างๆเพื่อใช้เป็นต้นทางในการส่ง Spam mail

72. ข้อใด<u>ไม่ใช่</u>ผลเสียที่เกิดจากการได้รับ Spam mail ที่มีจำนวนมาก
   a. ทำให้มี traffic จำนวนมากเกิดขึ้นในระบบ network จนอาจทำให้เครือข่ายล่มได้
   b. แฝงมาด้วย virus ที่ก่อให้เกิดความเสียหายแก่เครือข่ายและคอมพิวเตอร์
   c. ทำให้การทำงานของเครื่องช้าลง และมี service แปลกๆ run เพิ่มขึ้น
   D.องค์กรขาดความน่าเชื่อถือเนื่องจากส่ง spam mail ออกสู่ internet จนติด black list
   e. เปิดช่องทางให้แก่ hacker เข้ามาในเครือข่ายได้ผ่านทางช่องทางที่ spam mail สร้างขึ้น

73. ข้อใดเป็นการช่วยลดปริมาณ spam mail
a. ใช้ outlook ในการกรอง spam mail
b. ทำ mail relay system
c. หลีกเลี่ยงการอ่าน/ตอบ mail ที่ไม่รู้จักผู้ส่งหรือที่คาดว่าเป็น spam
d. ถูกทั้งข้อ a และ c
e. ถูกทั้งข้อ a, b และ c

74. ข้อใด<u>ไม่ใช่</u>ต้นเหตุที่ทำให้เกิด spam mail
a. พฤติกรรมการใช้งาน internet ของ user ในระบบ b. การทำ mail relay system
c. มีธุรกิจซื้อขายข้อมูล e-mail address d. ถูกทั้ง a และ c
e.ถูกทั้ง a, b และ c

75.เมื่อ user ได้รับ e-mail ที่เป็น spam ควรทำอย่างไร
a. เก็บ mail ฉบับนั้นไว้ใน junk folder
b. เปิดอ่าน mail ศึกษารายละเอียด เพื่อให้ทราบว่า spam มีลักษณะอย่างไร
c. แจ้ง administrator เพื่อสกัด e-mail ที่น่าสงสัย
d. ถูกทั้ง a และ b
e. ถูกทั้ง a และ c

Trojan

76. Trojan ที่เป็นประเภท VBSscript มีการทำงานอย่างไร
a. พยายามทำลายไฟล์ระบบของเครื่อง จนกระทั่งบูตไม่ได้
b. โจมตีเครื่องเป้าหมายและเผยแพร่ผ่าน e-mail Outlook Express เพื่อโจมตีหรือกระจายไวรัส
c. ใช้คำสั่งในการรันคำสั่งอื่นเพื่อทำลายระบบ หรือเปลี่ยนไฟล์
d. ถูกทั้ง a และ b
e. ถูกทั้ง b และ c

77. Trojan มีคุณสมบัติอย่างไร
a. คัดลอกตัวเองและส่งตัวเองไปยังเครื่องอื่นๆโดยไม่แพร่เชื้อไปติดไฟล์อื่น สร้างความเสียหายให้กับระบบเครือข่าย
b. ไม่สามารถส่งตัวเองไปยังเครื่องอื่นๆได้ ไม่แพร่เชื้อไปติดไฟล์อื่น สิ่งที่มันทำคือเปิดโอกาสให้ผู้ไม่ประสงค์ดีเข้ามาควบคุมเครื่องที่ติดเชื้อจากระยะไกล
c. ไม่สามารถส่งตัวเองไปยังคอมพิวเตอร์เครื่องอื่นๆ แพร่เชื้อไปติดไฟล์อื่นๆในคอมพิวเตอร์โดยการแนบตัวมันเองเข้าไป สร้างความเสียหายให้กับไฟล์
d. ไม่สามารถส่งตัวเองไปยังคอมพิวเตอร์เครื่องอื่นๆ ไม่แพร่เชื้อไปติดไฟล์อื่น สิ่งที่มันทำคือรบกวนและละเมิดความเป็นส่วนตัวของผู้ใช้
e. คัดลอกตัวเองและส่งตัวเองไปยังเครื่องอื่นๆ และแพร่เชื้อไปติดไฟล์อื่น ทำลายไฟล์

78. ลักษณะอาการตามข้อใดที่บ่งบอกว่าเครื่องติด Trojan
a. CD Drive มีการทำงานแปลกๆ เปิด/ปิด เอง b. ไฟล์บนเครื่องหายไปเองโดยไม่มีร่องรอย
c. ค่าที่กำหนดของวินโดวส์บางอย่างถูกแก้ไข d. ไม่มีข้อใดถูก
e. ถูกทุกข้อ

79. การกระทำในข้อใดมีความเสี่ยงที่ทำให้เครื่องคอมพิวเตอร์ติด Trojan
a. เปิดอ่าน e-mail ทุกฉบับ ที่เข้ามาใน mailbox
b. ไม่มีการ update patch และ service pack ของระบบปฏิบัติการ
c. ไม่มีการติดตั้ง firewall และเปิด port ที่ไม่จำเป็น
d. ถูกทั้งข้อ a และ b
e. ถูกทั้ง a, b และ c

80. เมื่อเครื่องคอมพิวเตอร์ติด Trojanสามารถค้นหาข้อมูลที่น่าเชื่อถือที่แนะนำการแก้ปัญหาได้จากที่ใด
a. ThaiCert b. SANS c. Pantip d. ถูกทั้ง a และ b
e. ถูกทั้ง b และ c

Bot Net หรือ Back door หรือ Root Kit

81.เมื่อเครื่องในเครือข่ายติด Bot net ทำให้ปัญหาในข้อใดเกิดตามมา
a. เครื่องคอมพิวเตอร์ส่งข้อมูลแปลกๆออกไปยังอินเตอร์เน็ต
b. ติด black list ว่าเป็นที่มาของการโจมตี server อื่นๆ
c. ISP ไม่สามารถให้บริการลูกค้าที่เป็น Bot net ได้

d. ไม่สามารถติดต่อสื่อสารผ่านอินเตอร์เน็ตได้ ทำให้เกิดความเสียหายทางธุรกิจ

e. ถูกทุกข้อ

82.ข้อใดเป็นการป้องกัน Bot net ในขั้นพื้นฐาน

a. ให้ความรู้ความเข้าใจแก่ผู้ใช้คอมพิวเตอร์ถึงภัยจาก Bot net b. การเปิดใช้งาน Personal Firewall

c. หมั่น Update Patch ด้วย Window Update d. ไม่มีข้อถูก

e. ถูกทั้ง a, b และ c

83.ข้อใดต่อไปนี้ไม่ใช่ความสามารถของ Rootkit

a. การได้สิทธิผู้ดูแลระบบ ทำให้สามารถควบคุมเครื่องได้หมดทันที

b. อนุญาติให้โปรแกรมบางโปรแกรมใช้งานตัว Rootkit ได้ เพื่อที่จะใช้ประโยชน์จากการซ่อนตัวของ Rootkit เอง

c. ปกปิดหรือยับยั้งการเข้าถึงโพรเซสที่เกี่ยวกับ การใช้งานของระบบ เช่น การดูโพรเซสการทำงาน , การแก้ไข Registry , การเปิดปิด พอร์ทที่ใช้งาน

d. ใช้เครื่องที่โดน Rootkit ในการโจมตีอื่นๆ เช่น ส่งอีเมล์ สแปมจำนวนมากออกไป

e. สามารถเกิดขึ้นได้ในระบบปฏิบัติการ linux เท่านั้น

84.มีบริษัทรายหนึ่งได้นำ rootkit มาใช้เพื่อให้เกิดประโยชน์ต่อองค์กร ข้อใดต่อไปนี้กล่าวได้ถูกต้อง

a. บริษัท แกรมมี่ ใช้ rootkit ในการ เก็บข้อมูลการฟังเพลงในเครื่องของลูกค้า

b. บริษัท โซนี่ ใช้ rootkit ในการป้องกันการ copy cd อย่างไม่ถูกต้อง

c. rootkit ที่ถูกใช้งานทำหน้าที่แค่ป้องกันการ copy ไม่สามารถเปิดช่องทางให้ Hacker ได้

d. rootkit ที่ถูกใช้งาน ไม่สามารถซ่อนตัวในระบบปฏิบัติการ windows ได้ แต่สามารถซ่อนตัวใน linux ได้

e. ถูกทั้งข้อ b และ c

85.ข้อใดที่ทำให้ hacker สามารถติดตั้ง backdoor ในเครื่อง หรือ ระบบได้

a. โปรแกรมที่ใช้ในเครื่องหรือระบบนั้นๆมีช่องโหว่ ที่ไม่ได้รับการ patch และ update

b. ในเครือข่าย WLAN อนุญาตให้มีการใช้งาน mode Adhoc

c. เครื่องติด worm ที่สามารถทำการติดตั้ง backdoor ได้

d. เปิดไฟล์เอกสาร ที่ไม่ทราบแหล่งที่มา ทำให้ติด Trojan ที่สามารถติดตั้ง backdoor ได้

e. ถูกทุกข้อ

กรณีศึกษา ปัญหาข้างต้น Virus/Spyware/Spam/Trojan/Bot Net/Back door ที่เคยเกิดจริง ผ่านเครือข่าย อินเทอร์เน็ต (ตอบคำถามข้อ 26-30)

ปัจจุบันเหล่าอาชญากรยุคไฮเทคในปัจจุบันกำลังใช้เทคนิคใหม่ที่เข้ามาแอบขโมยข้อมูลส่วนตัวของเราตลอดจนทำให้เงินออกจากกระเป๋าเราได้อย่างง่ายดาย โดยเฉพาะผู้ที่ใช้บริการอินเตอร์เน็ตแบงค์กิ้งอยู่ในเวลานี้ วิธีการที่เหล่าอาชญากรไฮเทคนิยมใช้ได้แก่วิธี "Phishing" และ ล่าสุดคือวิธี "Pharming" ซึ่งอันตรายและน่ากลัวกว่าเดิมหลายเท่า

สำหรับเทคนิคใหม่ที่เรียกว่า "Pharming" เหล่าอาชญากรไซเบอร์ใช้วิธีใหม่ที่แนบเนียน คือ การโจมตีไปที่ระบบ DNS Server ของบริษัท หรือ ผู้ให้บริการอินเตอร์เน็ต (ISP) โดยตรง โดยวิธีแฮกเข้าไปในระบบ DNS หรือ ไม่ก็ใช้วิธีการที่เรียกว่า DNS Hijacking หรือ Poisoning ทำให้ผู้ใช้บริการที่ตกเป็นเหยื่อคิดว่าได้เข้าไปใน URL ที่ถูกต้องจริงๆ แต่ปรากฏว่า URL นั้นได้ถูก "Redirect" ไปยัง Web Site ปลอมที่อาชญากรไซเบอร์ทำรอไว้ให้หลงเข้าไปติดกับดัก

อีกวิธีหนึ่งก็คือ การแฮกเข้าที่เครื่อง Client ตามบ้าน ซึ่งใช้อินเตอร์เน็ตความเร็วสูง หรือ Broadband Internet แล้วส่งโทรจันเช่น Trojan/BankAsh-A หรือ PWSteal.Banking.A เข้ามาดักรออยู่ ในเครื่องของเหยื่อโดยตรง โทรจันตัวนี้ถือว่าเป็นไวรัสคอมพิวเตอร์แบบหนึ่ง ซึ่งมันจะเข้าไปแก้ไขไฟล์ HOSTS ที่อยู่ใน Sub Directory c:\windows\system32\drivers\etc หรือ c:\winnt\systems\drivers\etc และ เพิ่มบรรทัดที่หลอกให้เหยื่อไปยัง URL ปรกติแต่ถูก "Redirect" ไปยัง Web Site ที่อาชญากรไซเบอร์เตรียมไว้ ที่โดนกันไปก็คือ ธนาคารต่างๆในต่างประเทศ Barclays Bank และ HSBC Bank เป็นต้น

การโจมตีด้วยวิธีการ "Pharming" นี้ เหยื่อจะสังเกตุได้ยากมาก หรือ เรียกได้ว่าแทบไม่รู้ตัวเลยก็ว่าได้ เพราะ URL ที่เข้าไปก็เหมือนกับของ Web Site จริงทุกประการ แต่เป็นกลลวงที่ระบบ DNS ทำให้เหยื่อเกิดความเข้าใจผิด

86.จากบทความข้างต้นข้อใดที่<u>ไม่ใช่</u>วิธีสังเกตุและป้องกันไม่ให้ตกเป็นเหยื่อการทำ pharming

a. หมั่นตรวจสอบไฟล์ Host ในเครื่อง อย่างสม่ำเสมอเพื่อหาสิ่งผิดปกติ

b. ซึ่งต้องใช้ Digital Certificate มาช่วยในการตรวจสอบการเข้าถึงระบบ
c. ทำการ update และ patch เครื่อง DNS Server
d. พยายามสังเกตุ e-mail และ ไม่ควรเปิด e-mail
e. หมั่นตรวจสอบละประเมินความเสี่ยงอยู่เสมอ

87. จุดมุ่งหมายของการทำ phishing และ pharming เหมือนกันอย่างไร
a. มีวิธีการและเทคนิคที่เหมือนกัน b. มีเป้าหมายที่เหมือนกันคือการขโมยข้อมูลส่วนตัว
c. จำนวน target ในแต่ละครั้ง d. ถูกทั้ง a และ b
e. ถูกทั้ง b และ c

88. ในการทำ pharming จำเป็นต้องอาศัยองค์ประกอบใดบ้าง
a. Vulnerability b. Trojan c. spam mail d. ถูกทั้ง a และ b e. ถูกทั้ง b และ c

89. จากปัญหาที่เกิดจากการทำ pharming ทำให้เกิดความเสียหายในด้านใด
a. ภาพลักษณ์และความเชื่อถือที่มีต่อ ธนาคาร ลดน้อยลง
b. มีคนนำเงินไปฝากธนาคารน้อยลง เพราะกลัวโดนทำ pharming
c. ลูกค้าธนาคาร หลีกเลี่ยงการทำธุรกรรมการเงินทางอินเตอร์เน็ต
d. ถูกทั้ง a และ c
e. ถูกทั้ง a, b และ c

90. ทำไมจึงมีการเรียกเทคนิคดังกล่าวว่า "pharming"
a. เทคนิคดังกล่าวมีการใช้ Trojan จำนวนมาก ซึ่งเปรียบเหมือนกับการทำฟาร์มเลี้ยงม้า
b. เทคนิคดังกล่าวมีการหลอกล่อเหยื่อให้มาติดกับได้เป็นจำนวนมาก
c. Hacker redirect เหยื่อไปยังเว็บที่เตรียมไว้เหมือนการทำฟาร์มเลี้ยงสัตว์
d. ถูกทั้ง a และ b
e. ถูกทั้ง b และ c

กรณีศึกษา ปัญหาด้าน Virus/Spyware/Spam/Trojan/Bot Net/Back door ที่เคยเกิดจริงผ่านเครือข่าย Network / WLAN (ตอบคำถาม 31-35)

ปัจจุบันนี้ในองค์กรต่างๆได้มีบริการ Wireless ซึ่งจำเป็นอย่างยิ่งที่จะต้องมีการออกแบบระบบให้รัดกุมและมีความปลอดภัย เพราะไม่เช่นนั้นแล้ว WLAN ที่มีอยู่ในองค์จะกลายเป็น backdoor ชั้นดีให้ Hacker เข้ามาอยู่ในระบบ network และได้รับ IP เช่นเดียวกับพนักงานในองค์กรได้อย่างง่ายดาย ซึ่งสิ่งที่ตามมาก็คือ ระบบ network ขององค์กรจะกลายเป็น botnet ที่ hacker สามารถใช้เป็นเครื่องมือในการโจมตี ไปยังเป้าหมายต่างๆได้ เช่น สั่งให้เครื่องทุกเครื่องส่ง email spam ไปทุกหนทุกแห่ง เข้าเวปต่างๆหรือทำ transaction ที่ผิดกฎหมายก็เป็นได้ เมื่อ Hacker เข้ามาอยู่ใน network แล้วก็จะฝังพวก Trojan หรือเครื่องมือต่างๆที่ สามารถ ขโมยข้อมูลส่วนตัวของพนักงานในองค์กร ไปใช้ประโยชน์ตามที่ต้องการ ทำให้เกิดความเสียหายทั้งขององค์กรและพนักงานเอง ซึ่งการโจมตี WLAN มีหลายวิธี เช่น *Rogue Access Point และ Ad-hoc Networks, Peer-to-Peer Attacks, Eavesdropping, Encryption Attack, Authentication Attack, MAC Spoofing, Management Interface Exploits, Man-In-The-Middle Attack, Denial of Service* เป็นต้น

91. วิธีการใด<u>ไม่ใช่</u>การป้องกัน WLAN จากการโจมตีของ hacker
a. เปลี่ยน Login ID และรหัสผ่านของอุปกรณ์และหลีกเลี่ยงการใช้ SNMP
b. ปิดกั้นการทำงานในโหมด Adhoc หรือ Peer-to-Peer
c. การตั้งชื่อและปกปิด SSID ของอุปกรณ์แม่ข่าย
d. ใช้งาน WEP Encryption
e. กำหนด channel ให้แตกต่างกัน เพื่อไม่ให้สัญญาณชนกัน (11,1,6)

92. การออกแบบเพื่อติดตั้งอุปกรณ์ WLAN ในเครือข่ายควรจะเป็นอย่างไร
a. จัดให้อยู่ใน DMZ เพื่อความปลอดภัย
b. จัดแบ่ง VLAN สำหรับ WLAN โดยเฉพาะเพื่อป้องกันการ Hack เข้าเครือข่ายผ่านทาง WLAN
c. หลีกเลี่ยงการจ่าย IP แบบ DHCP
d. ติดตั้ง Firewall ระหว่าง WLAN และเครือข่ายภายใน
e. ถูกทุกข้อ

93. ลักษณะการโจมตีแบบใดที่เน้นการ Tool scan wireless network เพื่อหาข้อมูลเข้าระบบ
a. Rogue Access Point b. Eavesdropping c. Management

Interface Exploits
d. Wireless Hijacking e. Peer-to-Peer Attacks

94. การโจมตีที่มีรูปแบบในการขัดขวามเครื่อง client ให้ไม่สามารถติดต่อกับ AP ได้ เพื่อที่จะทำการ spoof MAC ของ client นั้น เรียกรูปแบบการโจมตีนี้ว่าอย่างไร
a. Man-In-The-Middle Attack b. Authentication Attack
c. MAC Spoofing d. Ad-hoc Networks
e. Denial of Service

95. จากข้อมูลข้างต้นเมื่อระบบ WLAN ถูก โจมตีจะก่อให้เกิดความเสียหายอย่างไรตามมาบ้าง
a. ระบบภายในองค์กร กลายเป็น botnet เป็นเครื่องมือของ hacker
b. ส่ง spam mail ไปโจมตียังเครือข่ายอื่น
c. traffic ภายในองค์กรเพิ่มมากขึ้น
d. ทำให้เครือข่ายในองค์กรล่มเพราะโดนโจมตี
e. เป็นไปได้ทุกข้อที่กล่าวมา

ข้อสอบตั้งแต่ข้อ 96-100 บางข้อมีตัวเลือกที่ถูกต้องมากกว่าหนึ่ง (Choose X) ต้องเลือกให้ถูกทุกข้อถึงได้คะแนน

96. Which of the following ICMP options can provide useful diagnostic information to an experienced attacker?
a. echo-request
b. time-stamp request
c. info request
d. address mask request
e. address mask, info, time stamp and echo request

97. Which of the following would best describe the use of the nmap scanning tool?
a. To perform quick network mapping and service identification in a network
b. To look for web server vulnerabilities
c. To fingerprint the software versions of all FTP servers in a network
d. To inject false Layer 2 information into the network
e. To spawn a shell on a compromised web server

98. How can you differentiate between logging sources in a SYSLOG record?
a. Use TCP as the transport protocol rather than UDP.
b. Put in place IPSEC tunnels and QoS guarantees between server and device.
c. Use the facility tag within a SYSLOG message.
d. Switch off console logging on a device.
e. Increase the logging level to "debugging".

99. Which of the following protocols would you implement as part of the solution to protect against TCP hijacking?
a. Telnet with one-time-password authentication
b. IPsec-encrypted Telnet
c. SSH
d. HTTP
e. HTTPS
f. Telnet
g. SNMP

100. What authentication mechanism is used by SNMP version 3?

a. Clear-text community string
b. MD5 HMACs
c. SHA HMACs
d. DES-encrypted passwords
e. 3DES-encrypted passwords
f. One-time passwords