- Network Security -

"Questions you should answer before disaster strikes your exam."

1. จงอธิบายความหมาย เทคนิคที่ใช้ และตัวอย่างการนำหลักการต่อไปนี้มาใช้งาน

Confidentiality
ความหมาย :
หลักการดังกล่าวนำมาใช้แก้ปัญหาอะไร
เทคนิคที่นำมาใช้ :
ตัวอย่างการประยุกต์ใช้งาน :

Integrity
ความหมาย :
หลักการดังกล่าวนำมาใช้แก้ปัญหาอะไร
เทคนิคที่นำมาใช้ :
ตัวอย่างการประยุกต์ใช้งาน :

Availability
ความหมาย :
หลักการดังกล่าวนำมาใช้แก้ปัญหาอะไร
เทคนิคที่นำมาใช้ :
ตัวอย่างการประยุกต์ใช้งาน :

Authentication
ความหมาย :
หลักการดังกล่าวนำมาใช้แก้ปัญหาอะไร
เทคนิคที่นำมาใช้ :
ตัวอย่างการประยุกต์ใช้งาน :

Authorization
ความหมาย :
หลักการดังกล่าวนำมาใช้แก้ปัญหาอะไร
เทคนิคที่นำมาใช้ :
ตัวอย่างการประยุกต์ใช้งาน :

Accounting
ความหมาย :
หลักการดังกล่าวนำมาใช้แก้ปัญหาอะไร
เทคนิคที่นำมาใช้ :
ตัวอย่างการประยุกต์ใช้งาน :

Prevent
ความหมาย :
หลักการดังกล่าวนำมาใช้แก้ปัญหาอะไร
เทคนิคที่นำมาใช้ :
ตัวอย่างการประยุกต์ใช้งาน :

Detect
ความหมาย :
หลักการดังกล่าวนำมาใช้แก้ปัญหาอะไร
เทคนิคที่นำมาใช้ :
ตัวอย่างการประยุกต์ใช้งาน :

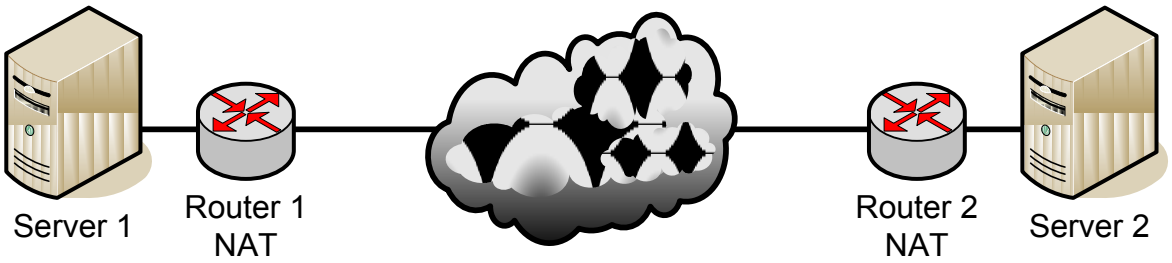
Respond
ความหมาย :
หลักการดังกล่าวนำมาใช้แก้ปัญหาอะไร
เทคนิคที่นำมาใช้ :
ตัวอย่างการประยุกต์ใช้งาน :

Access Control
ความหมาย :
หลักการดังกล่าวนำมาใช้แก้ปัญหาอะไร
เทคนิคที่นำมาใช้ :
ตัวอย่างการประยุกต์ใช้งาน :

2. เมื่อพิจารณาโปรแกรม Anti-Virus ต่างๆ ที่ทำงานในเชิง Detection System จงวิเคราะห์ว่าโปรแกรม Anti-Virus มีข้อมูลที่ใช้ตรวจสอบคืออะไร, ชนิดของการตรวจจับเป็นแบบใด, ระยะเวลาในการตอบสนองเป็นแบบไหน และผลลัพธ์ของการทำงานคืออะไร และในการทำงานของโปรแกรม Anti-Virus เหตุการณ์ใดทำให้เกิด False Positive และเหตุการณ์ใดทำให้เกิด False Negative และปัญหา False Alarm ทั้งสองกรณีจะแก้ไขได้อย่างไร

3. IP Security สามารถสร้างรูปแบบการเชื่อมต่อที่ทำได้ทั้ง Authentication และ Encryption พร้อมกันได้กี่รูปแบบ และทำได้อย่างไรบ้าง

4. เมื่อ Router 1 และ Router 2 มีการตั้งค่า Static NAT สำหรับ Server 1 และ Server 2 เนื่องจากเซิร์ฟเวอร์ทั้งสองไม่สามารถใช้ไอพีจริงได้ การตั้งค่าระบบให้ Server 1 และ Server 2 เชื่อมต่อกันโดยใช้ IP Security จะทำได้หรือไม่ หากทำได้จะทำได้โดยวิธีใด หากไม่สามารถทำได้จะไม่สามารถทำได้เนื่องจากสาเหตุใดและจะต้องปรับเปลี่ยนการออกแบบเครือข่ายและการตั้งค่าระบบอย่างไรจึงสามารถใช้งาน IP Security ได้



5. จงอธิบายกระบวนการทำ SQL Injection โดยละเอียด และแนะนำวิธีการป้องกันการโจมตีในลักษณะดังกล่าว

6. จงอธิบายกระบวนการทำ Cross Site Script โดยละเอียด และแนะนำวิธีการป้องกันการโจมตีในลักษณะดังกล่าว

7. ในการใช้งาน Wireless Network โดยใช้ Wireless Access Point ใน Home Office จะมีปัญหาความปลอดภัยอะไรบ้าง แต่ละปัญหามีวิธีการป้องกันได้อย่างไร และต้องตั้งค่าพารามิเตอร์เพื่อการป้องกันอย่างไร

8. กระบวนการ Direct-Server Return ในอุปกรณ์ Load Balancer ต้องมีการตั้งค่าระบบอย่างไร และกระบวนการดังกล่าวมีการส่งข้อมูลอย่างไร จงอธิบายโดยละเอียด

9. จงแสดงการหา Check Sum ขนาด 2 Bytes ของข้อมูลต่อไปนี้ “12 34 56 78 9A BC DE F0”

10. Digital Signature ที่สร้างขึ้นจาก Key ที่ไม่มี Certificate จะสามารถใช้งานได้ในระบบงานในลักษณะใดและจะไม่สามารถใช้งานได้ในงานในลักษณะใด จงให้เหตุผลประกอบ

11. การตั้งค่าระบบงานให้ทำงานแบบ High Availability กับการใช้ Load Balance มีวัตถุประสงค์การใช้งานที่แตกต่างกันอย่างไร และข้อดีข้อเสียของการทำงานทั้งสองแบบคืออะไร

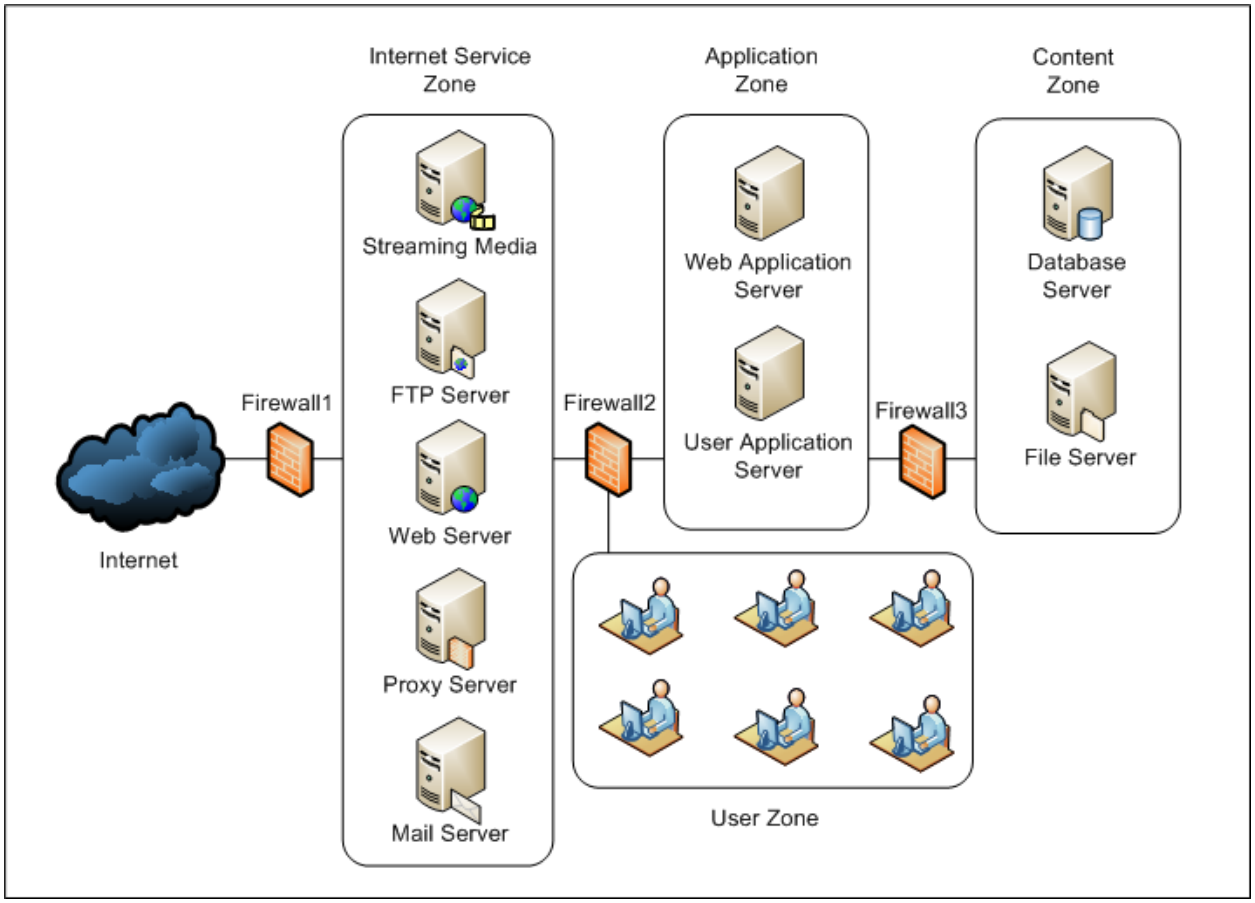
12. Incident Response Plan , Disaster Recovery Plan และ Business Continuity Plan ทั้งสามแผนมีวัตถุประสงค์การใช้งานอย่างไร และแต่ละแผนมีการใช้งานในสถานการณ์ใดบ้าง จงยกตัวอย่างให้เห็นชัดเจน

13. การทำ Authentication มีกี่รูปแบบ แต่ละแบบใช้หลักการอะไร จงยกตัวอย่างเครื่องมือหรือคุณลักษณะที่ใช้งานในแต่ละแบบ

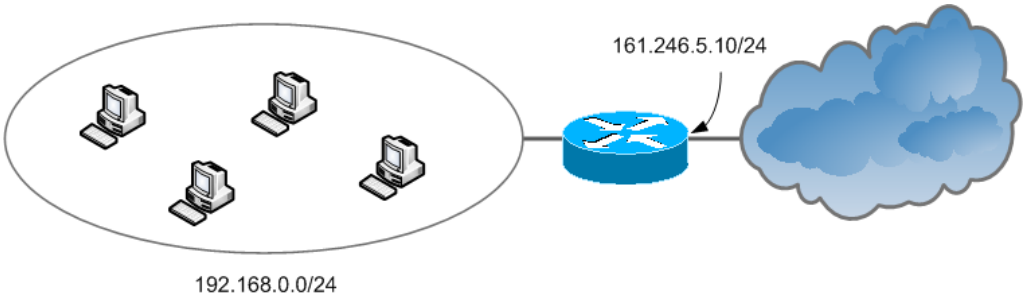
14. ปัญหาสำหรับผู้ใช้งาน social network เช่น facebook , twitter คืออะไรบ้างและการใช้ social network อย่างปลอดภัยมีหลักการอย่างไร

15. ให้นักศึกษาเขียนกฎกฎการคัดกรองต่างๆ ในอุปกรณ์ firewall แต่ละตัว โดย

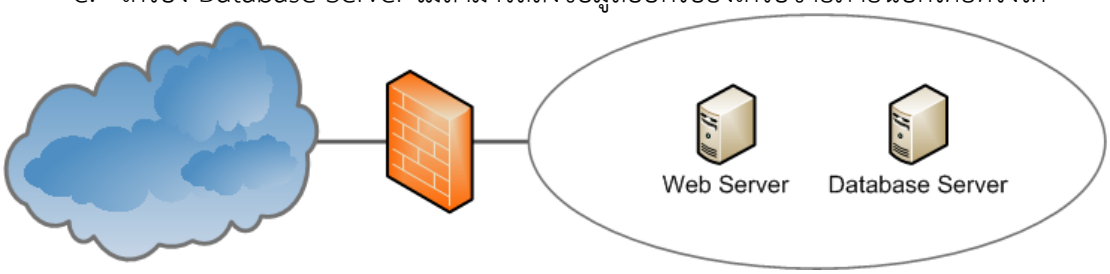
- เครือข่ายสมมุติคือเครือข่ายของบริษัทหนึ่ง ซึ่งมีผู้ใช้งานการใช้งาน 2 กลุ่มคือ กลุ่มผู้ใช้งานในอินเตอร์เน็ต และกลุ่มพนักงานในบริษัท
- ผู้ใช้งานในอินเตอร์เน็ตจะสามารถใช้งาน web ซึ่งมีทั้งข้อมูลที่ได้จากการประมวลผลผ่าน web application และข้อมูล video streaming สามารถส่งเมล์มายัง e-mail address ของบริษัทได้ และสามารถถ่ายโอนไฟล์สาธารณะต่างๆ ของบริษัทผ่าน ftp Server ได้
- กลุ่มพนักงานในบริษัทจะมีการติดตั้งโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลซึ่งจะเชื่อมต่อไปทำงาน application ต่างๆ ใน user application server และในการทำงานของพนักงาน จะมีการถ่ายโอนไฟล์เก็บใน file server ได้ ส่ง e-mail ผ่าน mail server ได้ และจะใช้งานอินเตอร์เน็ตผ่าน proxy server เท่านั้น
- ทั้ง web application server และ user application server จะใช้ข้อมูลในฐานข้อมูลเดียวกัน



16. จากเครือข่ายตัวอย่าง หากต้องการให้เครือข่าย 192.168.0.0/24 สามารถใช้งานอินเตอร์เน็ตได้ โดยใช้หมายเลข IP Address คือ 161.246.5.10/24 ต้องตั้งค่าอุปกรณ์เครือข่ายอย่างไร ตั้งค่า NAT Table และ ตั้งค่าทางเครือข่ายของเครื่องคอมพิวเตอร์ในเครือข่ายอย่างไร



17. จากเครือข่ายตัวอย่าง หากต้องการเพิ่มความปลอดภัยในเครือข่ายของเครื่องเซิร์ฟเวอร์ ต้องตั้งกฎใน Firewall อย่างไร โดยต้องการให้มีการทำงานได้ดังนี้
    a. เครือข่ายภายนอกใช้งานเว็บเซิร์ฟเวอร์ได้เฉพาะเปิดเว็บเท่านั้น
    b. เครือข่ายภายนอกสามารถ Ping ไปยังเครื่องเว็บเซิร์ฟเวอร์เท่านั้น
    c. เครือข่ายภายนอกไม่สามารถ Ping ไปยังเครื่อง Database Server ได้
    d. เครือข่ายภายนอกไม่สามารถติดต่อเครื่อง Database Server ได้
    e. เครื่อง Database Server ไม่สามารถส่งข้อมูลออกไปยังเครือข่ายภายนอกโดยตรงได้



18. ในหัวข้อ Web Application Security ให้นักศึกษาบอกปัญหาความปลอดภัยและการสร้างความปลอดภัยในแต่ละจุดต่อไปนี้

Web Browser :

ปัญหา	เทคนิคที่ใช้ในการสร้างความปลอดภัย

การเชื่อมต่อระหว่าง Web Browser กับ Web Server

ปัญหา	เทคนิคที่ใช้ในการสร้างความปลอดภัย

Web Server

ปัญหา	เทคนิคที่ใช้ในการสร้างความปลอดภัย

Database Server

ปัญหา	เทคนิคที่ใช้ในการสร้างความปลอดภัย

19. การส่งข้อมูลที่ขาด confidentiality จะเกิดปัญหาอะไร

20. การส่งข้อมูลที่ขาด integrity จะเกิดปัญหาอะไร

21. การโจมตีผ่านเครือข่ายต่อไปนี้มีลักษณะพิเศษของการโจมตีอย่างไร
    a. Syn Flood
    b. LAND Atack
    c. Fragmentation
    d. UDP Flood

22. Hashing Function ที่ดีต้องมีคุณสมบัติอย่างไร

23. จงอธิบายถึงสาเหตุที่ทำให้การใช้ Digital Signature มีความปลอดภัยมากกว่าการใช้ Message Authentication Code

24. จงอธิบายการทำงานของ Distributed Denial of Service (DDOS) และการป้องกันการโจมตีแบบ DDOS

25. อธิบายการทำงานของ Diffie-Hellman Key Exchange ว่ามีการทำงานอย่างไร พร้อมพิสูจน์ว่าผู้บุกรุกที่ดักจับข้อมูลระหว่างทางจะไม่สามารถทราบ Key ที่สร้างขึ้นได้

26. เมื่อกำหนด Key ในการเข้ารหัสแบบ AES แล้ว เราจะสามารถส่ง Key ที่สร้างขึ้น ไปยังปลายทางเพื่อถอดรหัสด้วยกระบวนการของ Diffie-Hellman Key Exchange ได้หรือไม่ เพราะเหตุใด

27. จงวาดแผนผังพร้อมอธิบายขั้นตอนการส่งข้อมูลจาก A ไปยัง B ที่ต้องการความปลอดภัยทั้งการรักษาความลับข้อมูล(Confidentiality) ,การตรวจสอบความถูกต้องของข้อมูล(Integrity) และไม่สามารถปฏิเสธความรับผิดชอบ(Non-reputation) ต้องมีขั้นตอนการดำเนินการที่ฝั่งรับและฝั่งส่งอย่างไร

28. ปัญหาด้าน Availability ของทรัพยากรต่อไปนี้คืออะไร และจะมีการป้องกันปัญหาดังกล่าวอย่างไร
    - หน่วยเก็บข้อมูล
    - CPU
    - ระบบเครือข่าย
    - หน่วยความจำ

29. การโจมตีทางเครือข่ายใดที่ Stateful Inspection Firewall สามารถป้องกันได้ แต่ Packet Filtering Firewall ไม่สามารถป้องกันได้ จงอธิบายลักษณะการทำงานของการโจมตีทางเครือข่ายดังกล่าว

30. หากสาขาวิชาต้องการปิดกั้นการใช้งานเว็บไซต์เครือข่ายสังคมเช่น Facebook , Twitter จะต้องใช้อุปกรณ์ Firewall ชนิดใด จงอธิบายวิธีการคัดกรองและยกตัวอย่างกฎการคัดกรอง

31. ในการออกแบบระบบ E-Commerce ควรมีการดำเนินการด้าน Confidentiality, Integrity, Availability, Authentication, Authorization และ Accounting ตรงส่วนใดบ้างของระบบ และแต่ละตำแหน่งจะดำเนินการโดยใช้เทคนิคหรือเทคโนโลยีอะไร