final exam cisco

Total points 28/73

final ที่กูแคปไว้เอง

✗ เหตุผลในการปิดการกระจายสัญญาณ SSID และการเปลี่ยน SSID ค่าเริ่มต้นบน wireless access point คืออะไร? *0/1

- การปิดการกระจายสัญญาณ SSID ช่วยเพิ่มแบนด์วิดท์ความถี่วิทยุและเพิ่มปริมาณข้อมูลที่ส่งผ่านของ access point
- ผู้ใช้ที่รู้ SSID ค่าเริ่มต้นสามารถเข้าถึง access point และเปลี่ยนการกำหนดค่าได้ ✗
- Access point หยุดการกระจาย MAC address ของตัวเอง ทำให้ป้องกันอุปกรณ์ไร้สายที่ไม่ได้รับอนุญาตเชื่อมต่อกับเครือข่าย
- อุปกรณ์ไร้สายจะต้องมีการกำหนดค่า SSID ด้วยตนเองเพื่อเชื่อมต่อกับเครือข่ายไร้สาย

Correct answer

- อุปกรณ์ไร้สายจะต้องมีการกำหนดค่า SSID ด้วยตนเองเพื่อเชื่อมต่อกับเครือข่ายไร้สาย

✗ เพื่อให้กระบวนการแก้ไขปัญหาง่ายขึ้น ข้อความ ICMP ขาเข้าแบบใดควรได้รับอนุญาตบนอินเตอร์เฟซภายนอก? *0/1

- time-stamp reply ✗
- echo reply
- echo request
- router advertisement
- time-stamp request

Correct answer

- echo reply

✗ บริการ syslog มีฟังก์ชันอะไรบ้าง? (เลือก 3 ข้อ) * 0/1

- [x] เพื่อให้สถิติเกี่ยวกับแพ็คเกตที่ไหลผ่านอุปกรณ์ Cisco ✗
- [ ] เพื่อให้การวิเคราะห์การจราจร
- [ ] เพื่อตรวจสอบตัวแทน (agents) เป็นระยะสำหรับข้อมูล
- [ ] เพื่อระบุปลายทางของข้อความที่จับได้
- [ ] เพื่อเลือกประเภทของข้อมูลการบันทึกที่จะจับ
- [ ] เพื่อรวบรวมข้อมูลการบันทึกสำหรับการตรวจสอบและแก้ไขปัญหา

Correct answer

- [x] เพื่อระบุปลายทางของข้อความที่จับได้
- [x] เพื่อเลือกประเภทของข้อมูลการบันทึกที่จะจับ
- [x] เพื่อรวบรวมข้อมูลการบันทึกสำหรับการตรวจสอบและแก้ไขปัญหา

ผลลัพธ์ใน self zone คืออะไร หากเราเตอร์เป็นต้นทางหรือปลายทางของการรับส่งข้อมูล? *0/1

- การรับส่งข้อมูลทั้งหมดได้รับอนุญาต
- เฉพาะการรับส่งข้อมูลที่มุ่งไปยังเราเตอร์เท่านั้นที่ได้รับอนุญาต
- **เฉพาะการรับส่งข้อมูลที่เริ่มต้นจากเราเตอร์เท่านั้นที่ได้รับอนุญาต** ✗
- ไม่อนุญาตการรับส่งข้อมูลใดๆ

Correct answer

- **การรับส่งข้อมูลทั้งหมดได้รับอนุญาต**

ช่างเทคนิคได้ติดตั้งโปรแกรมจากบุคคลที่สามที่ใช้จัดการคอมพิวเตอร์ Windows 7 อย่างไรก็ตาม โปรแกรมไม่เริ่มทำงานโดยอัตโนมัติเมื่อคอมพิวเตอร์เริ่มทำงาน ช่างเทคนิคควรทำอย่างไรเพื่อแก้ไขปัญหานี้? *0/1

- ถอนการติดตั้งโปรแกรมแล้วเลือก Add New Programs ในเครื่องมือ Add or Remove Programs เพื่อติดตั้งแอปพลิเคชัน
- ใช้เครื่องมือ Add or Remove Programs เพื่อตั้งค่าการเข้าถึงโปรแกรมและค่าเริ่มต้น
- เปลี่ยนประเภทการเริ่มต้นสำหรับโปรแกรมเป็น Automatic ใน Services
- **ตั้งค่าคีย์รีจิสทรีของแอปพลิเคชันเป็นหนึ่ง** ✗

Correct answer

- **เปลี่ยนประเภทการเริ่มต้นสำหรับโปรแกรมเป็น Automatic ใน Services**

คำสำคัญใดสองคำที่สามารถใช้ใน access control list เพื่อแทนที่ wildcard mask หรือ address และคู่ wildcard mask? (เลือก 2 ข้อ) *0/1

- [ ] qt
- [ ] host
- [x] any ✓
- [ ] all
- [ ] some
- [x] most ✗

Correct answer

- [x] host
- [x] any

✗ ข้อยกเว้นการเปิดเผยสามข้อใดที่เกี่ยวข้องกับ FOIA? (เลือก 3 ข้อ) * 0/1

- (●) ข้อมูลที่ระบุว่าไม่ได้รับการยกเว้นโดยกฎหมาย ✗
- ( ) ข้อมูลทางธุรกิจที่เป็นความลับ
- ( ) ข้อมูลสาธารณะจากสถาบันการเงิน
- ( ) ข้อมูลความมั่นคงแห่งชาติและนโยบายต่างประเทศ
- ( ) บันทึกการบังคับใช้กฎหมายที่เกี่ยวข้องกับข้อกังวลที่ระบุไว้
- ( ) ข้อมูลที่ไม่ใช่ทางธรณีวิทยาเกี่ยวกับบ่อน้ำ

Correct answers

- (●) ข้อมูลทางธุรกิจที่เป็นความลับ
- (●) ข้อมูลความมั่นคงแห่งชาติและนโยบายต่างประเทศ
- (●) บันทึกการบังคับใช้กฎหมายที่เกี่ยวข้องกับข้อกังวลที่ระบุไว้

✓ องค์กรอนุญาตให้พนักงานทำงานจากที่บ้านสองวันต่อสัปดาห์ ควรใช้เทคโนโลยีใดเพื่อให้มั่นใจว่าข้อมูลที่ส่งมีความลับ? *1/1

- (●) VPN ✓
- ( ) SHS
- ( ) RAID
- ( ) VLANS

✓ คุณได้รับการขอให้ดำเนินโปรแกรมความสมบูรณ์ของข้อมูลเพื่อปกป้องไฟล์ข้อมูลที่จำเป็นต้องดาวน์โหลดทางอิเล็กทรอนิกส์โดยพนักงานขาย คุณได้ตัดสินใจใช้อัลกอริทึม hashing ที่แข็งแกร่งที่สุดที่มีอยู่ในระบบของคุณ คุณจะเลือกอัลกอริทึม hash ใด? *1/1

- ( ) SHA-1
- ( ) MD5
- ( ) AES
- (●) SHA-256 ✓

✓ มาตรฐานไร้สายใดที่ทำให้ AES และ CCM เป็นข้อบังคับ? * 1/1

- ( ) WEP
- ( ) WPA
- ( ) WEP2
- (●) WPA2 ✓

✓ อะไรคือเป้าหมายของการโจมตีแบบ SQL injection? * 1/1

- ○ DHCP
- ○ DNS
- ○ email
- ◉ database ✓

✗ พารามิเตอร์ไร้สายใดที่ใช้โดย access point เพื่อกระจาย frames ที่รวม SSID? * 0/1

- ○ passive mode
- ○ security mode
- ○ channel setting
- ◉ active mode ✗

Correct answer

- ◉ passive mode

✓ วิธีใดที่สามารถใช้ในการเสริมความแข็งแกร่งให้กับอุปกรณ์? * 1/1

- ○ อนุญาตให้มีการตรวจจับ USB อัตโนมัติ
- ○ อนุญาตให้บริการเริ่มต้นยังคงเปิดใช้งาน
- ◉ ใช้ SSH และปิดการเข้าถึงบัญชี root ผ่าน SSH ✓
- ○ รักษาการใช้รหัสผ่านเดิม

✗ ข้อความใดอธิบายวิธีการตรวจจับการบุกรุกแบบ anomaly-based? * 0/1

- ◉ เปรียบเทียบลายเซ็นของการรับส่งข้อมูลขาเข้ากับฐานข้อมูลการบุกรุกที่รู้จัก ✗
- ○ เปรียบเทียบ antivirus ของโปรแกรมกับพื้นที่เก็บข้อมูลบนคลาวด์เพื่อรับการอัปเดตล่าสุด
- ○ เปรียบเทียบการทำงานของโฮสต์กับนโยบายความปลอดภัยที่กำหนดไว้อย่างชัดเจน
- ○ เปรียบเทียบพฤติกรรมของโฮสต์กับเส้นฐานที่กำหนดไว้เพื่อระบุการบุกรุกที่อาจเกิดขึ้น

Correct answer

- ◉ **เปรียบเทียบพฤติกรรมของโฮสต์กับเส้นฐานที่กำหนดไว้เพื่อระบุการบุกรุกที่อาจเกิดขึ้น**

✓ ขั้นตอนใดใน Vulnerability Management Life Cycle ที่ทำรายการสินทรัพย์ทั้งหมดในเครือข่ายและระบุรายละเอียดของโฮสต์ รวมถึงระบบปฏิบัติการและบริการที่เปิด? *1/1

- (●) discover ✓
- ( ) remediate
- ( ) assess
- ( ) prioritize assets

✗ IMAP สามารถเป็นภัยคุกคามความปลอดภัยต่อบริษัทได้อย่างไร? * 0/1

- (●) มีคนคลิกบน hidden iFrame โดยไม่ได้ตั้งใจ ✗
- ( ) มันสามารถใช้เข้ารหัสข้อมูลที่ถูกขโมยและส่งไปยังผู้ที่คุกคาม
- ( ) อีเมลสามารถใช้นำมัลแวร์มาสู่โฮสต์ได้
- ( ) ข้อมูลที่เข้ารหัสถูกถอดรหัส

Correct answer

- (●) อีเมลสามารถใช้นำมัลแวร์มาสู่โฮสต์ได้

✗ อะไรคือประโยชน์ 3 ประการของการใช้ symbolic links มากกว่า hard links ใน Linux? (เลือก 3 ข้อ) *0/1

- [x] พวกมันสามารถเชื่อมโยงไปยังไดเรกทอรี ✓
- [x] พวกมันสามารถเชื่อมโยงไปยังไฟล์ในระบบไฟล์ที่แตกต่างกัน ✓
- [x] พวกมันสามารถเข้ารหัสได้ ✗
- [ ] พวกมันสามารถบีบอัดได้
- [ ] พวกมันสามารถแสดงตำแหน่งของไฟล์ต้นฉบับ
- [ ] Symbolic links สามารถส่งออกได้

Correct answer

- [x] พวกมันสามารถเชื่อมโยงไปยังไดเรกทอรี
- [x] พวกมันสามารถเชื่อมโยงไปยังไฟล์ในระบบไฟล์ที่แตกต่างกัน
- [x] พวกมันสามารถแสดงตำแหน่งของไฟล์ต้นฉบับ

✗ เครื่องมือใดสองอย่างที่มีอินเตอร์เฟซ GUI และสามารถใช้ดูและวิเคราะห์การจับแพ็คเกตแบบเต็มได้? (เลือก 2 ข้อ) *0/1

- [x] Splunk ✗
- [ ] tcpdump
- [ ] nfdump
- [x] Wireshark ✓
- [ ] Cisco Prime Network Analysis Module

Correct answer

- [x] Wireshark
- [x] Cisco Prime Network Analysis Module

✗ อะไรคือหลักการของโมเดลการควบคุมการเข้าถึงแบบ nondiscretionary? * 0/1

- (●) มันใช้การควบคุมการเข้าถึงที่เข้มงวดที่สุดเท่าที่จะเป็นไปได้ ✗
- ( ) มันอนุญาตให้การตัดสินใจเข้าถึงขึ้นอยู่กับบทบาทและความรับผิดชอบของผู้ใช้ภายในองค์กร
- ( ) มันอนุญาตให้เข้าถึงตามคุณลักษณะของวัตถุที่จะเข้าถึง
- ( ) มันอนุญาตให้ผู้ใช้ควบคุมการเข้าถึงข้อมูลของพวกเขาในฐานะเจ้าของข้อมูลนั้น

Correct answer

- (●) มันอนุญาตให้การตัดสินใจเข้าถึงขึ้นอยู่กับบทบาทและความรับผิดชอบของผู้ใช้ภายในองค์กร

✗ อะไรคือตัวอย่างของการโจมตีแบบ local exploit? * 0/1

- (●) การโจมตีแบบ buffer overflow ถูกเปิดตัวต่อเว็บไซต์ช้อปปิ้งออนไลน์และทำให้เซิร์ฟเวอร์ล่ม ✗
- ( ) การสแกนพอร์ตถูกใช้เพื่อกำหนดว่าบริการ Telnet กำลังทำงานบนเซิร์ฟเวอร์ระยะไกลหรือไม่
- ( ) ผู้คุกคามดำเนินการโจมตีแบบ brute force บนเราเตอร์ขอบขององค์กรเพื่อให้ได้รับการเข้าถึงที่ผิดกฎหมาย
- ( ) ผู้คุกคามพยายามที่จะได้รับรหัสผ่านผู้ใช้ของโฮสต์ระยะไกลโดยใช้ซอฟต์แวร์จับคีย์บอร์ดที่ติดตั้งบนเครื่องโดย Trojan

Correct answer

- (●) ผู้คุกคามพยายามที่จะได้รับรหัสผ่านผู้ใช้ของโฮสต์ระยะไกลโดยใช้ซอฟต์แวร์จับคีย์บอร์ดที่ติดตั้งบนเครื่องโดย Trojan

✗ เพื่อให้แน่ใจว่าห่วงโซ่การควบคุมถูกรักษาไว้ สิ่งใดสามอย่างควรถูกบันทึกเกี่ยวกับหลักฐานที่ถูกเก็บรวบรวมและวิเคราะห์หลังจากที่เกิดเหตุการณ์ด้านความปลอดภัย? (เลือก 3 ข้อ) *0/1

- [x] หมายเลขซีเรียลและชื่อโฮสต์ของอุปกรณ์ที่ใช้เป็นหลักฐาน ✓
- [ ] เวลาและวันที่ที่หลักฐานถูกเก็บรวบรวม
- [x] ช่องโหว่ที่ถูกใช้ประโยชน์ในการโจมตี ✗
- [ ] มาตรการที่ใช้เพื่อป้องกันเหตุการณ์
- [x] ตำแหน่งของหลักฐานทั้งหมด ✓
- [ ] ขอบเขตของความเสียหายต่อทรัพยากรและสินทรัพย์

Correct answer

- [x] หมายเลขซีเรียลและชื่อโฮสต์ของอุปกรณ์ที่ใช้เป็นหลักฐาน
- [x] เวลาและวันที่ที่หลักฐานถูกเก็บรวบรวม
- [x] ตำแหน่งของหลักฐานทั้งหมด

✓ เมื่อโปรไฟล์เซิร์ฟเวอร์สำหรับองค์กรกำลังถูกสร้างขึ้น องค์ประกอบใดอธิบายถึง TCP และ UDP daemons และพอร์ตที่ได้รับอนุญาตให้เปิดบนเซิร์ฟเวอร์? *1/1

- ( ) critical asset address space
- (•) listening ports ✓
- ( ) service accounts
- ( ) software environment

✓ อะไรที่บ่งบอกโดย Snort signature ID ที่ต่ำกว่า 3464? * 1/1

- (•) SID ถูกสร้างโดย Sourcefire และถูกเผยแพร่ภายใต้ข้อตกลง GPL ✓
- ( ) SID ถูกสร้างโดยชุมชน Snort และถูกรักษาไว้ใน Community Rules
- ( ) นี่เป็นลายเซ็นที่กำหนดเองที่พัฒนาโดยองค์กรเพื่อแก้ไขกฎที่สังเกตเห็นในท้องถิ่น
- ( ) SID ถูกสร้างโดยสมาชิกของ EmergingThreats

หลังจากที่โฮสต์ A ได้รับหน้าเว็บจากเซิร์ฟเวอร์ B โฮสต์ A ยกเลิกการเชื่อมต่อกับเซิร์ฟเวอร์ B จับคู่แต่ละตัวเลือกกับขั้นตอนที่ถูกต้องในกระบวนการยกเลิกปกติสำหรับการเชื่อมต่อ TCP *

	Step 1	Step 2	Step 3	Step 4	Score	
Server B sends ACK to Host A	○	◉	○	○	1/1	✓
Server B sends FIN to Host A	◉	○	○	○	0/1	✗
Host A sends ACK to Server B	○	○	◉	○	0/1	✗
Host A sends FIN to Server B	○	○	○	◉	0/1	✗

Correct answers

	Step 1	Step 2	Step 3	Step 4
Server B sends FIN to Host A	○	○	◉	○
Host A sends ACK to Server B	○	○	○	◉
Host A sends FIN to Server B	◉	○	○	○

✓ ผู้ดูแลเครือข่ายกำลังตั้งค่าเว็บเซิร์ฟเวอร์สำหรับสำนักงานโฆษณาขนาดเล็กและกังวลเกี่ยวกับความพร้อมใช้งานของข้อมูล ผู้ดูแลต้องการใช้งานการทนต่อความผิดพลาดของดิสก์โดยใช้จำนวนดิสก์น้อยที่สุดที่จำเป็น ผู้ดูแลควรเลือก RAID ระดับใด? *1/1

- ○ RAID 0
- ○ RAID 5
- ◉ RAID 1 ✓
- ○ RAID 6

จับคู่แท็บของ Windows 10 Task Manager กับฟังก์ชันของมัน *

	Services	Startup	Details	Performance	Score	
อนุญาตให้กระบวนการมีการตั้งค่า affinity ของมัน	○	○	◉	○	1/1	✓
อนุญาตให้โปรแกรมที่กำลังทำงานเมื่อเริ่มต้นระบบถูกปิดการใช้งาน	○	◉	○	○	1/1	✓
อนุญาตให้เริ่มหยุด หรือเริ่มต้นใหม่ของบริการเฉพาะ	◉	○	○	○	1/1	✓
แสดงข้อมูลการใช้ทรัพยากรสำหรับ CPU, หน่วยความจำ, เครือข่าย, ดิสก์ และอื่นๆ	○	○	○	◉	1/1	✓

✗ ข้อความใดอธิบายการทำงานของ Cisco IOS Zone-Based Policy Firewall? * 0/1

- ○ การกระทำ pass ทำงานในทิศทางเดียวเท่านั้น
- ○ อินเตอร์เฟซการจัดการเราเตอร์ต้องถูกกำหนดเองไปยังโซน self
- ○ นโยบายบริการถูกใช้ในโหมดการกำหนดค่าอินเตอร์เฟซ
- ◉ อินเตอร์เฟซเราเตอร์สามารถอยู่ในหลายโซนได้ ✗

Correct answer

- ◉ การกระทำ pass ทำงานในทิศทางเดียวเท่านั้น

จับคู่ลำดับขั้นตอนที่ถูกต้องที่ผู้คุกคามมักจะใช้ในการโจมตีแบบ domain shadowing *

	Step 1	Step 2	Step 3	Step 4	Step 5	Score	
An exploit kit landing page is created	◉	○	○	○	○	0/1	✗
The website is compromised	○	◉	○	○	○	0/1	✗
HTTP 302 cushioning is used	○	○	◉	○	○	0/1	✗
Domain shadowing is used	○	○	○	○	◉	0/1	✗
Malware is spread through its payload	○	○	○	◉	○	0/1	✗

Correct answers

	Step 1	Step 2	Step 3	Step 4	Step 5
An exploit kit landing page is created	○	○	○	◉	○
The website is compromised	◉	○	○	○	○
HTTP 302 cushioning is used	○	◉	○	○	○
Domain shadowing is used	○	○	◉	○	○
Malware is spread through its payload	○	○	○	○	◉

✗ ในความพยายามที่จะป้องกันการโจมตีเครือข่าย นักวิเคราะห์ไซเบอร์แชร์คุณลักษณะที่ระบุได้เฉพาะของการโจมตีที่รู้จักกับเพื่อนร่วมงาน คุณลักษณะหรือตัวบ่งชี้การบุกรุกประเภทใดสามอย่างที่มีประโยชน์ในการแชร์? (เลือก 3 ข้อ) *0/1

- [x] ชื่อ netbios ของไฟร์วอลล์ที่ถูกบุกรุก ✗
- [x] คุณลักษณะของไฟล์มัลแวร์ ✓
- [ ] BIOS ของระบบที่โจมตี
- [ ] การเปลี่ยนแปลงที่ทำกับซอฟต์แวร์ระบบปลายทาง
- [ ] ID ระบบของระบบที่ถูกบุกรุก
- [x] ที่อยู่ IP ของเซิร์ฟเวอร์โจมตี ✓

Correct answer

- [x] คุณลักษณะของไฟล์มัลแวร์
- [x] การเปลี่ยนแปลงที่ทำกับซอฟต์แวร์ระบบปลายทาง
- [x] ที่อยู่ IP ของเซิร์ฟเวอร์โจมตี

✗ บริการใดสามอย่างที่มีโดย FireEye? (เลือก 3 ข้อ) * 0/1

- [ ] ระบุและหยุดมัลแวร์แฝงบนไฟล์
- [x] ใช้งานชุดกฎการตรวจจับเหตุการณ์ไปยังเครื่องมือความปลอดภัยเครือข่าย ✗
- [x] บล็อกการโจมตีทั่วเว็บ ✓
- [ ] สร้างกฎไฟร์วอลล์แบบไดนามิก
- [ ] ระบุและหยุดเวกเตอร์การคุกคามทางอีเมล
- [x] ข้อมูลการจราจรทั้งหมดผ่านการวิเคราะห์แพ็คเกตเชิงลึก ✗

Correct answer

- [x] ระบุและหยุดมัลแวร์แฝงบนไฟล์
- [x] บล็อกการโจมตีทั่วเว็บ
- [x] ระบุและหยุดเวกเตอร์การคุกคามทางอีเมล

✓ อะไรคือลักษณะของการวิเคราะห์ความน่าจะเป็นในการประเมินการแจ้งเตือน? * 1/1

- ( ) แต่ละเหตุการณ์เป็นผลที่หลีกเลี่ยงไม่ได้ของสาเหตุก่อนหน้า
- ( ) วิธีการที่แม่นยำซึ่งให้ผลลัพธ์เดียวกันทุกครั้งโดยอาศัยเงื่อนไขที่กำหนดไว้ล่วงหน้า
- ( ) การวิเคราะห์แอปพลิเคชันที่เป็นไปตามมาตรฐานแอปพลิเคชัน/เครือข่าย
- (•) ตัวแปรสุ่มที่สร้างความยากลำบากในการรู้ผลลัพธ์ของเหตุการณ์ที่กำหนดด้วยความแน่นอน ✓

✓ อุปกรณ์ใดจะถูกใช้เป็นแนวป้องกันที่สามในแนวทางการป้องกันเชิงลึก (defense-in-depth)? *1/1

- firewall
- host
- internal router ✓
- edge router

✗ เมื่อใช้งาน ZPF การตั้งค่าความปลอดภัยเริ่มต้นเมื่อส่งต่อการจราจรระหว่างสองอินเตอร์เฟซในโซนเดียวกันคืออะไร? *0/1

- การจราจรระหว่างอินเตอร์เฟซในโซนเดียวกันถูกส่งต่ออย่างเลือกสรรตามข้อมูล Layer 3 ✗
- การจราจรระหว่างอินเตอร์เฟซในโซนเดียวกันไม่ขึ้นอยู่กับนโยบายใดๆ และผ่านอย่างอิสระ
- การจราจรระหว่างอินเตอร์เฟซในโซนเดียวกันถูกบล็อก
- การจราจรระหว่างอินเตอร์เฟซในโซนเดียวกันถูกส่งต่ออย่างเลือกสรรตามข้อจำกัดนโยบายเริ่มต้น

Correct answer

- การจราจรระหว่างอินเตอร์เฟซในโซนเดียวกันไม่ขึ้นอยู่กับนโยบายใดๆ และผ่านอย่างอิสระ

✗ โดเมนความปลอดภัยคลาวด์ใดอธิบายการควบคุมที่เกี่ยวข้องกับการรักษาความปลอดภัยของข้อมูลเอง? *0/1

- Infrastructure Security ✗
- Security as a Service
- Data Security and Encryption
- Application Security

Correct answer

- Data Security and Encryption

✗ บริษัทกำลังใช้ผู้ให้บริการคลาวด์สาธารณะเพื่อโฮสต์กระบวนการพัฒนาและการแจกจ่ายซอฟต์แวร์ ทรัพยากรคลาวด์สองอย่างใดที่บริษัทมีความรับผิดชอบเพียงผู้เดียวในโมเดลความรับผิดชอบความปลอดภัยร่วมกัน? (เลือก 2 ข้อ) *0/1

- [ ] network control
- [x] identity management ✗
- [ ] application
- [ ] data
- [x] customer endpoints ✓

Correct answer

- [x] data
- [x] customer endpoints

✗ องค์กรกำลังพัฒนาโปรแกรมการกำกับดูแลข้อมูลที่เป็นไปตามระเบียบข้อบังคับและนโยบาย บทบาทใดในโปรแกรมนี้มีหน้าที่รับผิดชอบในการตรวจสอบการปฏิบัติตามนโยบายและขั้นตอน กำหนดการจัดประเภทที่เหมาะสมให้กับสินทรัพย์ข้อมูล และกำหนดเกณฑ์สำหรับการเข้าถึงสินทรัพย์ข้อมูล? *0/1

- (•) data protection officer ✗
- ( ) data owner
- ( ) data controller
- ( ) data custodian

Correct answer

- (•) data owner

✓ บริษัทหนึ่งจัดการข้อมูลลูกค้าที่มีความอ่อนไหวสำหรับลูกค้าหลายราย กลไกการยืนยันตัวตนในปัจจุบันเพื่อเข้าถึงฐานข้อมูลคือชื่อผู้ใช้และวลีรหัสผ่าน บริษัทกำลังทบทวนความเสี่ยงของการรั่วไหลของข้อมูลประจำตัวพนักงานที่อาจนำไปสู่การรั่วไหลของข้อมูลและตัดสินใจดำเนินการเพื่อลดความเสี่ยงก่อนที่จะดำเนินการเพิ่มเติมเพื่อกำจัดความเสี่ยง บริษัทควรดำเนินการใดในตอนนี้? *1/1

- (•) **ใช้การยืนยันตัวตนแบบหลายปัจจัย** (multi-factor authentication) ✓
- ( ) ติดตั้งเครื่องสแกนลายนิ้วมือหรือจอประสาทตา
- ( ) ซื้อกรมธรรม์ประกันภัย
- ( ) เพิ่มประสิทธิภาพการเข้ารหัสข้อมูลด้วยอัลกอริธึมขั้นสูง

✓ องค์กรด้านความปลอดภัยใดที่รักษารายการช่องโหว่และการเปิดเผยทั่วไป (CVE) และใช้โดยองค์กรด้านความปลอดภัยชั้นนำ? *1/1

- (●) MITRE ✓
- ( ) SecurityNewsWire
- ( ) SANS
- ( ) CIS

✗ Diamond Model ของการวิเคราะห์การบุกรุกช่วยนักวิเคราะห์ความปลอดภัยไซเบอร์อย่างไร? *0/1

- (●) โดยการถ่ายทอดคุณสมบัติทั่วไปและความรุนแรงของช่องโหว่การบุกรุกในระบบคอมพิวเตอร์ฮาร์ดแวร์และซอฟต์แวร์ ✗
- ( ) โดยการแสดงให้เห็นว่าผู้โจมตีเปลี่ยนจากเหตุการณ์การบุกรุกหนึ่งไปยังอีกเหตุการณ์หนึ่งอย่างไร
- ( ) โดยการติดตามขั้นตอนของเหตุการณ์การบุกรุกตั้งแต่ขั้นตอนการสำรวจในช่วงแรกจนถึงการดึงข้อมูลออก
- ( ) โดยการแสดงให้เห็นถึงยุทธวิธี เทคนิค และขั้นตอน (TTP) ซึ่งเป็นส่วนหนึ่งของการป้องกันการบุกรุกและการระบุตัวผู้กระทำ

Correct answer

- (●) **โดยการแสดงให้เห็นว่าผู้โจมตีเปลี่ยนจากเหตุการณ์การบุกรุกหนึ่งไปยังอีกเหตุการณ์หนึ่งอย่างไร**

จับคู่บริการข่าวกรองภัยคุกคามกับคำอธิบาย *

	MITRE Corporation	FireEye	Cisco Talos	DHS Automated Indicator Sharing	Score	
blocks attacks across the web and email threat vectors, and latent malware that resides on file shares	○	◉	○	○	0/0	✗
creates and maintains a catalog of known security threats called Common Vulnerabilities and Exposures (CVE)	○	○	◉	○	0/0	✗
provides a real-time exchange of cyber threat indicators between the U.S. Government and the private sector	◉	○	○	○	0/0	✗
collects information about active, existing, and emerging threats and provides comprehensive protection against these attacks to subscribers	○	○	○	◉	0/0	✗

Correct answers

	MITRE Corporation	FireEye	Cisco Talos	DHS Automated Indicator Sharing
blocks attacks across the web and email threat vectors, and latent malware that resides on file shares	○	○	◉	○
creates and maintains a catalog of known security threats called Common Vulnerabilities and Exposures (CVE)	◉	○	○	○
provides a real-time exchange of cyber threat	○	○	○	◉

indicators between the U.S. Government and the private sector	
collects information about active, existing, and emerging threats and provides comprehensive protection against these attacks to subscribers	○ ◉ ○ ○

✓ การควบคุมประเภทใดช่วยค้นพบภัยคุกคามที่อาจเกิดขึ้นใหม่? * 1/1

- ○ Preventive controls
- ○ Corrective controls
- ◉ Detective controls ✓

✗ นักวิเคราะห์ความปลอดภัยไซเบอร์กำลังทดสอบเครื่องสแกนช่องโหว่ใหม่บนระบบ นักวิเคราะห์เลือกที่จะรันการสแกนที่ก้าวก่ายระบบโดยใช้ข้อมูลประจำตัว (intrusive credentialed scan) ไม่กี่นาทีต่อมา ระบบที่รันการสแกนล่มสลาย อะไรคือสาเหตุที่เป็นไปได้มากที่สุดของการล่มสลาย? *0/1

- ◉ a false negative ✗
- ○ a false positive
- ○ the intrusive scan
- ○ a hardware failure

Correct answer

- ◉ the intrusive scan

จับคู่เครื่องมือคำสั่งบรรทัดคำสั่ง (command line tool) กับฟังก์ชันของมัน *

	ifconfig	hping	netcat	nbistat	nmap	Score	
ใช้เพื่อรวบรวมข้อมูลจากการเชื่อมต่อเครือข่าย TCP และ UDP และยังสามารถใช้สำหรับการสแกนพอร์ตการตรวจสอบ การจับแบนเนอร์และการคัดลอกไฟล์	○	◉	○	○	○	0/1	✗
ใช้ในระบบปฏิบัติการ Mac/Linux เพื่อแสดงการตั้งค่า TCP/IP (ที่อยู่ IP, subnet mask, default gateway, DNS, และข้อมูล MAC)	◉	○	○	○	○	1/1	✓
ใช้เพื่อช่วยแก้ไขปัญหาการแก้ไขชื่อ NetBIOS ในระบบ Windows	○	○	◉	○	○	0/1	✗
ใช้ในการประกอบและวิเคราะห์แพ็คเก็ต และใช้สำหรับการสแกนพอร์ตการค้นหาเส้นทาง การระบุระบบปฏิบัติการและการทดสอบไฟร์วอลล์	○	○	○	○	◉	0/1	✗
ใช้ในการตรวจสอบความปลอดภัย มันระบุตำแหน่งโฮสต์เครือข่าย ตรวจจับระบบปฏิบัติการ และระบุบริการ	○	○	○	◉	○	0/1	✗

Correct answers

	ifconfig	hping	netcat	nbistat	nmap
ใช้เพื่อรวบรวมข้อมูลจากการ	○	○	◉	○	○

เชื่อมต่อเครือข่าย TCP และ UDP และยังสามารถใช้สำหรับการสแกนพอร์ต การตรวจสอบการจับแบนเนอร์ และการคัดลอกไฟล์					
ใช้เพื่อช่วยแก้ไขปัญหาการแก้ไขชื่อ NetBIOS ในระบบ Windows	○	○	○	◉	○
ใช้ในการประกอบและวิเคราะห์แพ็คเก็ต และใช้สำหรับการสแกนพอร์ต การค้นหาเส้นทาง การระบุระบบปฏิบัติการ และการทดสอบไฟร์วอลล์	○	◉	○	○	○
ใช้ในการตรวจสอบความปลอดภัย มันระบุตำแหน่งโฮสต์เครือข่าย ตรวจจับระบบปฏิบัติการ และระบุบริการ	○	○	○	○	◉

✓ นักวิเคราะห์ความเสี่ยงทำการวิเคราะห์ความเสี่ยงเชิงปริมาณและพบว่าปัจจัย SLE (Single Loss Expectancy - ความคาดหวังการสูญเสียครั้งเดียว) คือ $10,000 และปัจจัย ARO (Annualized Rate of Occurrence - อัตราการเกิดขึ้นรายปี) คือ 10% ปัจจัย ALE (Annualized Loss Expectancy - ความคาดหวังการสูญเสียรายปี) จะเป็นเท่าไรจากค่าเหล่านี้? *1/1

- ◉ $1,000 ✓
- ○ $150
- ○ $100
- ○ $1,500

✗ ภัยคุกคามทางไซเบอร์ประเภทใดที่จะทำให้เกิดไฟฟ้าดับ? * 0/1

- sabotage
- utility interruption
- human error
- ✗ hardware failure

Correct answer

- utility interruption

✓ การมีมุมมองแคบ ตู้ ATM บรรเทาการโจมตีประเภทใด? * 1/1

- ✓ shoulder surfing
- identity fraud
- quid pro quo
- dumpster diving

✗ ผู้โจมตีกำลังใช้การโจมตีแบบ Smurf เพื่อทำให้เครื่องเป้าหมายล้น ภัยคุกคามนั้นเป็นแบบใด? *0/1

- amplification and reflection attack
- UDP flood attack
- ✗ TCP SYN flood attack
- MAC address spoofing attack

Correct answer

- amplification and reflection attack

✗ นักศึกษากำลังเรียนรู้เกี่ยวกับโปรโตคอลการยืนยันตัวตนและวิธีการใช้สื่อสารกับเซิร์ฟเวอร์ AAA ข้อความใดอธิบายลักษณะของโปรโตคอลดังกล่าว? *0/1

- ✗ **RADIUS ใช้การท้าทายและตอบสนองแบบสองทิศทาง (CHAP) ในขณะที่ TACACS+ ใช้การท้าทายแบบทิศทางเดียว**
- TACACS+ รวมการยืนยันตัวตนและการอนุญาตเข้าใช้ ในขณะที่ RADIUS แยก AAA ตามสถาปัตยกรรม AAA
- TACACS+ เป็นมาตรฐานที่อุปกรณ์ Cisco ส่วนใหญ่รองรับ ในขณะที่ RADIUS เป็นมาตรฐานเปิด
- RADIUS ถือว่าเป็นโปรโตคอลที่ปลอดภัยกว่าเพราะการแลกเปลี่ยนโปรโตคอล RADIUS ทั้งหมดถูกเข้ารหัส

Correct answer

- **TACACS+ เป็นมาตรฐานที่อุปกรณ์ Cisco ส่วนใหญ่รองรับ ในขณะที่ RADIUS เป็นมาตรฐานเปิด**

✗ อะไรคือคุณสมบัติของ Windows 10 ที่เข้ารหัสไดรฟ์ที่ถอดได้? * 0/1

- (●) MRT ✗
- ( ) BitLocker To Go
- ( ) XProtect
- ( ) Leafpad

Correct answer

- (●) BitLocker To Go

✗ ความจำเป็นของความสมบูรณ์ของข้อมูล (data integrity) ในฟอรั่มและหน้าส่วนตัว บนโซเชียลมีเดียคืออะไร? *0/1

- (●) low ✗
- ( ) critical
- ( ) mid
- ( ) high

Correct answer

- (●) high

✗ นักวิเคราะห์ความปลอดภัยไซเบอร์ต้องระบุแง่มุมสามประการใดขององค์กรก่อนที่จะพัฒนานโยบายความปลอดภัยที่ครอบคลุม? *0/1

- [ ] security budget
- [ ] potential threats
- [x] system vulnerabilities ✓
- [ ] organization assets
- [ ] the type of network data traffic
- [x] the placement of firewalls ✗

Correct answer

- [x] potential threats
- [x] system vulnerabilities
- [x] organization assets

✓ อะไรคือปัจจัยสำคัญที่ทำให้ระบบอุตสาหกรรมและระบบฝังตัวมีความเสี่ยงสูง? * 1/1

- ระบบเหล่านี้จำนวนมากได้ถูกติดตั้งใช้งานแล้ว ซึ่งหมายความว่าการนำความปลอดภัยมาใช้เป็นเรื่องที่ยุ่งยากและใช้เวลานาน
- ระบบเหล่านี้มักมีจุดการเข้าถึงเพื่อการบริหารจัดการจำนวนมาก
- **อุปกรณ์จำนวนมากในระบบเหล่านี้มีการยืนยันตัวตนที่ไม่ดีและไม่สามารถอัปเกรดหรือแพตช์ได้** ✓
- การปรับปรุงความปลอดภัยของระบบที่มีต้นทุนต่ำเหล่านี้จะเพิ่มค่าใช้จ่ายมากเกินไป

✗ อะไรที่ใช้โดยเกตเวย์ชั้นแอปพลิเคชัน (application layer gateway) เพื่อเชื่อมต่อกับเซิร์ฟเวอร์ระยะไกลในนามของไคลเอนต์? *0/1

- packet filter
- intrusion detection system ✗
- stateful firewall
- proxy server

Correct answer

- proxy server

✗ เทคนิคใดช่วยให้สามารถควบคุมความปลอดภัยของการจราจรและเวิร์กโฟลว์ภายในคลาวด์ได้อย่างละเอียดมากขึ้น? *0/1

- Zone-based Policy Firewalls ✗
- AAA
- WPA2-AES encryption
- microsegmentation

Correct answer

- microsegmentation

✓ กลไกความปลอดภัยใดที่ให้การเข้ารหัสข้อมูล ยืนยันความถูกต้องของข้อมูล และรับประกันว่าข้อมูลไม่เปลี่ยนแปลงระหว่างการส่งผ่าน? *1/1

- IPsec ✓
- AAA
- digital signatures
- multi-factor authentication

✗ อะไรคือตัวอย่างของข้อมูลธุรกรรมที่บันทึกโดยเครื่องมือตรวจสอบความปลอดภัยเครือข่าย? *0/1

- (●) หมายเลขพอร์ตต้นทางและปลายทางของจุดปลายทางเครือข่ายสองจุด ✗
- ( ) ที่อยู่ IP ต้นทางและปลายทางของจุดปลายทางเครือข่ายสองจุด
- ( ) รหัส IP สำหรับโปรโตคอลที่ใช้
- ( ) คำขอและการตอบกลับระหว่างจุดปลายทางเครือข่ายสองจุด

Correct answer

- (●) คำขอและการตอบกลับระหว่างจุดปลายทางเครือข่ายสองจุด

✓ ทำไมเซิร์ฟเวอร์ Syslog ของเครือข่ายอาจเป็นเป้าหมายสำหรับผู้ก่อภัยคุกคาม? * 1/1

- (●) เซิร์ฟเวอร์ Syslog อาจมีข้อมูลที่อาจนำไปสู่การตรวจพบการโจมตีโดยแฮกเกอร์ ✓
- ( ) ข้อมูล Syslog อาจถูกเข้ารหัสโดยผู้โจมตีและใช้เป็นมัลแวร์เรียกค่าไถ่ (ransomware)
- ( ) เซิร์ฟเวอร์ Syslog มีการกำหนดค่าและรหัสผ่านสำหรับอุปกรณ์ทั้งหมดบนเครือข่าย
- ( ) เซิร์ฟเวอร์ Syslog มักไม่ได้ติดตั้งอยู่หลังไฟร์วอลล์

✓ การยืนยันตัวตน (authentication) และการอนุญาต (authorization) ให้ฟังก์ชันอะไรเพื่อจัดการการเข้าถึงทรัพยากรและบริการเครือข่าย? *1/1

- (●) การยืนยันตัวตนคือการตรวจสอบตัวตนของผู้ใช้ และการอนุญาตคือการกำหนดว่าผู้ใช้นั้นสามารถเข้าถึงบริการใดได้ ✓
- ( ) เมื่อผู้ใช้ผ่านกระบวนการยืนยันตัวตน การเข้าถึงทรัพยากรเครือข่ายที่ได้รับอนุญาตจะเป็นไปโดยอัตโนมัติ
- ( ) การยืนยันตัวตนและการอนุญาตเป็นขั้นตอนที่ไม่จำเป็นในการใช้กระบวนการ AAA
- ( ) การยืนยันตัวตนคือการกำหนดว่าผู้ใช้สามารถเข้าถึงบริการใดได้ และการอนุญาตคือการตรวจสอบตัวตนของผู้ใช้

✓ วิศวกรความปลอดภัยเครือข่ายกำลังตรวจสอบการกำหนดค่าไฟร์วอลล์นโยบายตามโซน (Zone-based Policy Firewall) บนเราเตอร์ Cisco และสังเกตเห็นผลลัพธ์ต่อไปนี้: *1/1

policy-map type inspect PRIV-TO-PUB-POLICY

class type inspect HTTP-TRAFFIC

inspect

class class-default

drop

อะไรคือวัตถุประสงค์ของคำสั่ง class class-default และ drop ในส่วนการกำหนดค่านี้?

- มันจะใช้การควบคุมการจราจรแบบที่อิงสถานะ (stated-based traffic control) กับการจราจรเริ่มต้นที่ได้รับอนุญาตให้ผ่านระหว่างโซนที่ระบุ
- มันช่วยให้มั่นใจว่ามีการบันทึกการจราจรทั้งหมดของคลาสการจราจรที่ระบุ
- **มันจะทำให้การจราจรทั้งหมดที่ไม่ได้เป็นสมาชิกของคลาสการจราจรที่ระบุถูกทิ้ง (drop)** ✓
- มันจะใช้นโยบายความปลอดภัยเริ่มต้นกับสมาชิกคลาสการจราจรที่ระบุ

✓ ทำไม ACLs (Access Control Lists) อาจให้ความรู้สึกปลอดภัยที่ไม่ถูกต้องหากพึ่งพามากเกินไปในฐานะเทคโนโลยีความปลอดภัยเครือข่าย? *1/1

- ACLs สามารถนำไปใช้กับอินเตอร์เฟซเครือข่ายในทิศทางเดียวเท่านั้น
- **ผู้โจมตีสามารถระบุได้ว่าที่อยู่ IP โปรโตคอล และพอร์ตใดที่ได้รับอนุญาตโดย ACLs** ✓
- แพ็คเก็ตจะได้รับอนุญาตโดยค่าเริ่มต้นเมื่อคำสั่ง ACL ไม่ตรงกัน
- ACLs บันทึกเฉพาะการจราจรที่ถูกปฏิเสธ ไม่ใช่การจราจรที่ได้รับอนุญาต