ชอัตนัย

1. **Security Ethics** คือ… professional practice ..something..

2. ISO 27001 ปีล่าสุดมีกี่ domain
Answer:

ถ้าหมายถึง **ISO 27001:2013 มี 14 domains, 114 controls**
เวอร์ชั่นก่อนหน้า ISO 27001:2005 มี 11 domains, 133 controls

http://practicalinfosec.wordpress.com/2013/10/08/the-new-iso-27001/
http://www.slideshare.net/mpsinghrathore/mapping-of-iso-270012005-with-iso-270012013

3. sniffing ผิดมาตราใด
Answer:

มาตรา ๘ ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้
ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์
และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคล
ทั่วไปใช้ประโยชน์ได้ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

4. ถังดับเพลิง type ใด ดับคอม
Answer:

ถังดับเพลิงชนิดผงเคมีแห้ง และ ถังดับเพลิงชนิดCO2
ใช้ดับไฟ ประเภท C
เป็นสัญลักษณ์รูปตัว C ในวงกลมสีฟ้าสามารถดับไฟที่เกิดจากเชื้อเพลิงที่มีลักษณะเป็นของแข็ง หรือมีกระแสไฟฟ้าไหลอยู่ เช่น อุปกรณ์ไฟฟ้าทุกชนิด

https://th.wikipedia.org/wiki/%E0%B8%96%E0%B8%B1%E0%B8%87%E0%B8%94%E0%B8%B1%E0%B8%9A%E0%B9%80%E0%B8%9E%E0%B8%A5%E0%B8%B4%E0%B8%87

5. RAID … is Stripping
Answer:

RAID 0 - Striping
RAID 1 - Mirroring
RAID 2 - Bit-level Striping with Dedicated Hamming-code Parity
RAID 3 - Byte-level Striping with Dedicated Parity
RAID 4 - Block-level Striping with Dedicated Parity
RAID 5 - Block-level Striping with Distributed Parity
RAID 6 - Block-level Striping with Double Distributed Parity

https://en.wikipedia.org/wiki/RAID#Standard_levels

6. Malware that encryption file for money
Answer:

Ransomware

https://en.wikipedia.org/wiki/Ransomware_%28malware%29

7. wget เว็บ www.test.com ด้วยยูสเซอร์ user1 รหัส pass
Answer

wget --user user1 --password=pass www.test.com

8. เขียน filter wireshark เพื่อกรอง access point ที่มี mac address aa:bb:cc:dd:ee:ff
Answer:
wlan.bssid eq aa:bb:cc:dd:ee:ff

https://www.wireshark.org/docs/dfref/w/wlan.html

9. ใช้ tcpdump ทำ sniffer ที่ interface eth2 จากต้นทาง 1.2.3.4 ถึงปลายทาง 1.2.3.5
Answer:
tcpdump -i eth2 src 1.2.3.4 and dst 1.2.3.5

http://www.danielmiessler.com/study/tcpdump/

10. ใช้ nc ทำ port scanning ไอพี 1.2.3.4 ตั้งแต่ port 1 ถึง 65535
Answer:
nc -v 61.91.8.232 -z 1-65535

ปรนัย

cobit เวอร์ชั่นล่าสุด?
choices: [5],5.1,4,4.1
iis log location
login error log location
fm200,h2o effect
choices: fiber optic พัง, คอมพัง, คนตาย
business continuity plan
TTL ใน icmp used for ?

datacenter backup site characteristic
backup link between branch
แมลงที่มีผลต่อ datacenter
choices: แมงสาบ, แมงมุม, มด, ?
พรบ ที่เกี่ยวข้องกับไอที มีกี่ฉบับ
case study พนักงาน it ในองค์กร
หัวหน้าบอกให้ลง photoshop เถื่อนทำไง?
choices: ทำเพราะหัวหน้ารับผิดชอบ
หัวหน้าบอกให้ลบภาพโป๊ในคอมทำงาน
choices: ทำเพราะผิดกฎหมาย
พนักงานองค์กรเจอ flash drive มีข้อมูลลูกค้าบ.อื่นทำไง?
choices: บอกหัวหน้า, บอกผู้บริหาร, บอกตำรวจ, บอกเพื่อนใน fb
bcm มาจาก ISO/BS อะไร
itil มาจาก ISO/BS อะไร
ตรวจสอบเวอร์ชั่น router cisco
choice: snmp

owasp attack example : direct obj ref,broken access control, missing function level AC
web app attack example : cookie poisoning,session hijack, xss
[^ ให้ http header มาเป็น http:// มี cookie PHPSESSION, GET params เต็มไปหมด]
ใส่ <script>alert('tnsc')</script> ในหน้าสมัครเป็นการทดสอบโจมตีแบบ xss
การโจมตีใดไม่จำเป็นต้องถอดรหัสข้อมูล replay
relation botnet-zombie
compare hacker,cracker
relation attacker,defender : work alone,not alone
penetration testing phase :recon,scan...
จัดการกับ risk ที่ impact สูง,เกิดบ่อย ด้วยวิธีใด
choice: risk avoid/transfer/accept/change
ข้อใด compromise integrity เช่น readmail
ถ้า admin audit ระบบตัวเองแล้วไม่เจอช่องโหว่หมายความว่า server นั้นปลอดภัยหรือไม่
ช่vuln ที่ไม่ public ถือเป็น risk หรือไม่
ข้อใดเป็นระบบที่ปลอดภัย
choice : robust system , xxx , xx
good ids host-base สามารถป้องกนทั้งเนผ เน็ตเวิร์คเลยหรือไม่

ข้อใดต้องคำนึงน้อยที่สุดสำหรับ data center,ห้องควบคุม
choices: ความชื้น, อุณหภูมิ, กระแสไฟฟ้า, ?
ข้อใดไม่ควรทำกับ data center
choices: บนพื้น raise floor 20m, กำแพงกระจกหันหน้าเข้าแดดเพื่อระบายความชื้น,พื้น

amazon ec2 … (something) …

มาตรฐานซอฟต์แวร์ CMMI

ip v6 มีกี่ address 3.4 * 10^38
ip v6 advantage over[2^128] ipv4

block SMB port ? tcp/udp? 135,136,137,445?

IPsec VPN กับ SSL VPN ต่างกันยังไง?
choices: ssl site to site, ipsec remote access
backup site อยู่ห่างกี่กม.
ความสัมพันธ์ระหว่าง disaster recovery กับ high availability
เอกสาร ISO27001 หลายข้อ application of …
เอกสาร ISO27001 สิ่งที่ต้องทำอย่างแรก…
computer fraud ส่วนมากเกิดจาก
choices: man-in-the-browser
fraud เกิดจาก การเงิน กดดันการทำงาน

dumpster diving อยู่ phase ไหน
choices: recon
ระบบตรวจสอบการโจทตีคืออันไหน :SEM(SIEM) มั้ง
ข้อมดแ็ เป็นห่ การโจมตีที่ไม่ใช่ application layer : slowloris,ping
กรณีเห็น package ping เป็นจำนวนมากคาดว่าสาเหตุเกิดจากอะไร
การ scan เข้าหมายสามารถใช้เทคนิคใด : ping scan,ping sweep

buff[6] string ="1234556678" strcpy(buff,string) overflow แบบใด heap,stack

ใช้ nmap สแกนซอฟต์แวร์เวอร์ชั่น
choices: -sV -F, -A -T4
ใช้ nmap สแกนระบบปฏิบัติการณ์
choices: -O
class ไหนมี host 254 เครื่อง
choices: a,b,c,d
กฎหมายใดเกี่ยวข้องกับ uninet โดยตรง
กฎหมายใดเกี่ยวข้องกับการจัดสอบโดยตรง
กฎหมายใดเกี่ยวข้องกับมหาวิทยาลัยโดยตรง
กฎหมายใดเกี่ยวข้องกับคนไทยในชีวิตประจำวัน
กฎหมายใดมีผลกับคนไทยนอกราชอาณาจักร
choices: พรบ.คอม,พรบ.ธุรกรรมอิเล็ก,กฎหมายลิขสิทธิ์
apt ย่อมาจาก advanced persistent threat

root.exe?/c+dir in which environment

choices: Windows/Linux + IIS/Apache

NSA สอดแนมคนใน USA?
choices: ทำได้ เพราะถูกกฎหมาย
NSA สอดแนมผู้นำประเทศในยุโรป?
choices: ผิดกฎหมายเพราะไม่ใช่ USA

##
##

อัตนัย

1**. Security Ethics** คือ… professional practice ..something..

2. ISO 27001 ปีล่าสุดมีกี่ domain

Answer:
ถ้าหมายถึง **ISO 27001:2013 มี 14 domains, 114 controls**
เวอร์ชั่นก่อนหน้า ISO 27001:2005 มี 11 domains, 133 controls
http://practicalinfosec.wordpress.com/2013/10/08/the-new-iso-27001/
http://www.slideshare.net/mpsinghrathore/mapping-of-iso-270012005-with-iso-270012013

3. sniffing ผิดมาตราใด

Answer: **มาตรา ๘**
ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคล

ทั่วไปใช้ประโยชน์ได้ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

4. **ถังดับเพลิง type ใด ดับคอม**

Answer: **ถังดับเพลิงชนิดผงเคมีแห้ง และ ถังดับเพลิงชนิด CO2**

ใช้ดับไฟ ประเภท C เป็นสัญลักษณ์รูปตัว C
ในวงกลมสีฟ้าสามารถดับไฟที่เกิดจากเชื้อเพลิงที่มีลักษณะเป็นของแข็ง หรือมีกระแสไฟฟ้าไหลอยู่ เช่น อุปกรณ์ไฟฟ้าทุกชนิด
https://th.wikipedia.org/wiki/%E0%B8%96%E0%B8%B1%E0%B8%87%E0%B8%94%E0%B8%B1%E0%B8%9A%E0%B9%80%E0%B8%9E%E0%B8%A5%E0%B8%B4%E0%B8%87

5. **RAID … is Stripping**

Answer: **RAID 0 - Striping**
RAID 1 - Mirroring
RAID 2 - Bit-level Striping with Dedicated Hamming-code Parity
RAID 3 - Byte-level Striping with Dedicated Parity
RAID 4 - Block-level Striping with Dedicated Parity
RAID 5 - Block-level Striping with Distributed Parity
RAID 6 - Block-level Striping with Double Distributed Parity
https://en.wikipedia.org/wiki/RAID#Standard_levels

6. **Malware that encryption file for money**

Answer: **Ransomware**
https://en.wikipedia.org/wiki/Ransomware_%28malware%29

7. **wget เว็บ www.test.com ด้วยยูสเซอร์ user1 รหัส pass**
Answer **wget --user user1 --password=pass www.test.com**

8. **เขียน filter wireshark เพื่อกรอง access point ที่มี mac address aa:bb:cc:dd:ee:ff**
Answer: **wlan.bssid eq aa:bb:cc:dd:ee:ff**
https://www.wireshark.org/docs/dfref/w/wlan.html

9. **ใช้ tcpdump ทำ sniffer ที่ interface eth2 จากต้นทาง 1.2.3.4 ถึงปลายทาง 1.2.3.5**
Answer: **tcpdump -i eth2 src 1.2.3.4 and dst 1.2.3.5**
http://www.danielmiessler.com/study/tcpdump/

10. **ใช้ nc ทำ port scanning ไอพี 1.2.3.4 ตั้งแต่ port 1 ถึง 65535**
Answer: **nc -v 61.91.8.232 -z 1-65535**

ปรนัย

Network Security Concept

- Vuln ที่ไม่ public ถือเป็น risk หรือไม่
- compare hacker,cracker

- relation attacker,defender : work alone,not alone
- Botnet กับ Zombie เกี่ยวข้องกันอย่างไร
    1. Zombie คือเทคนิคการใช้ เครื่องหลาย ๆ เครื่อง ที่ติด botnet แล้วใช้ในการโจมตีเครื่องอื่นผ่าน
        เครือข่าย
    2. Botnet คือเทคนิคการใช้ เครื่องหลาย ๆ เครื่อง ที่ติด Zombie แล้วใช้ในการโจมตีเครื่องอื่นผ่าน
        เครือข่าย
    3. Botnet และ Zombie ไม่เกี่ยวข้องกัน
    4. Botnet คือการใช้เครื่องเดียวในการโจมตีเครื่องอื่นผ่านเครือข่าย
    5. ผิดทุกข้อ
- ข้อใด compromise integrity เช่น readmail

Network Security Architecture

- Good ids host-base สามารถป้องกันทั้งเน็ตเวิร์คเลยหรือไม่
- ข้อใดเป็นระบบที่ปลอดภัย
    Choice: robust system, xxx, xx
- IPsec VPN กับ SSL VPN ต่างกันยังไง?
    Choices: SSL site to site, IPSec remote access

Network Security Assessment & Penetration Test Method

- TTL ใน icmp ถูกใช้ในการทดสอบเพื่อ?
- ใช้ nmap สแกนซอฟต์แวร์เวอร์ชั่น
    Choices: -sV -F, -A -T4
- ใช้ nmap สแกนระบบปฏิบัติการณ์
    Choices: -O
- Dumpster diving อยู่ phase ไหน

Choices: recon

• การ scan เป้าหมายสามารถใช้เทคนิคใด : ping scan, ping sweep

• ถ้า admin audit ระบบตัวเองแล้วไม่เจอช่องโหว่หมายความว่า server นั้นปลอดภัยหรือไม่

• ตรวจสอบเวอร์ชั่น router cisco

Choice: snmp

• ข้อใดเป็นขั้นตอนในการตรวจสอบช่องโหว่ด้วยวิธีการเจาะระบบ

1. Reconnaissance, scanning, gaining access, covering, clearing tracks, and installing back doors
2. Reconnaissance, scanning, gaining access, maintaining access, covering, clearing tracks, and installing back doors
3. Reconnaissance, scanning, gaining access, maintaining access, malicious activity
4. Reconnaissance, social engineering, scanning, maintaining access, gaining access

• OWASP attack example: direct obj ref, broken access control, missing function level AC

• [^ ให้ http header มาเป็น http:// มี cookie PHPSESSION, GET params เต็มไปหมด]

• Web app attack example: cookie poisoning, session hijack, xss

• ใส่ <script>alert('tnsc')</script> ในหน้าสมัครเป็นการทดสอบโจมตีแบบ xss

• การโจมตีใดไม่จำเป็นต้องถอดรหัสข้อมูล replay

Network Security Monitoring

• IIS log location

• Login error log location

• กรณีเห็น package ping เป็นจำนวนมากคาดว่าสาเหตุเกิดจากอะไร

• One of the following is not part of “monitor system health”, which one?

1. Monitor system load
2. Monitor memory
3. Monitor disk space
4. Monitor network performance
5. Monitor flow-capture

ISO 27001 and series

• Cobit เวอร์ชั่นล่าสุด?

Choices: [5], 5.1, 4, 4.1

• เอกสาร ISO27001 หลายข้อ application of …

• เอกสาร ISO27001 สิ่งที่ต้องทำอย่างแรก…

• BCM มาจาก ISO/BS อะไร: BS 25999

• ITIL มาจาก ISO/BS อะไร: ISO/IEC 20000 (previously BS15000)ISO/S 25999e, IPSหตุเกิดจากอะ

Computer Laws

• พรบ ที่เกี่ยวข้องกับไอที มีกี่ฉบับ

• กฎหมายใดเกี่ยวข้องกับ uninet โดยตรง

• กฎหมายใดเกี่ยวข้องกับการจัดสอบโดยตรง

• กฎหมายใดเกี่ยวข้องกับมหาวิทยาลัยโดยตรง

• กฎหมายใดเกี่ยวข้องกับคนไทยในชีวิตประจำวัน

• กฎหมายใดมีผลกับคนไทยนอกราชอาณาจักร

Choices: พรบ.คอม, พรบ.ธุรกรรมอิเล็ก, กฎหมายลิขสิทธิ์

• NSA สอดแนมคนใน USA?

Choices: ทำได้ เพราะถูกกฎหมาย

• NSA สอดแนมผู้นำประเทศในยุโรป?

Choices: ผิดกฎหมายเพราะไม่ใช่ USA

(มีเกี่ยวกับ พรบ ต่างๆ เช่น ลิขสิทธ์, การทำธุรกรรมอิเล็กทรอนิก)

Governance Risk and Compliance

Computer Security Ethics (Case Study)

• Case study พนักงาน it ในองค์กร
• หัวหน้าบอกให้ลง Photoshop เถื่อนทำไง?
    Choices: ทำเพราะหัวหน้ารับผิดชอบ
• หัวหน้าบอกให้ลบภาพโป๊ในคอมทำงาน
    Choices: ทำเพราะผิดกฎหมาย
• พนักงานองค์กรเจอ flash drive มีข้อมูลลูกค้าบ.อื่นทำไง?
    Choices: บอกหัวหน้า, บอกผู้บริหาร, บอกตำรวจ, บอกเพื่อนใน fb

IT Security Risk Management (Case Study)

• ระบบตรวจสอบการโจทตีคืออันไหน :SEM(SIEM)
    Security information management (SIM) and security event manager (SEM)
• ความสัมพันธ์ระหว่าง disaster recovery กับ high availability
• ข้อใดเป็นวิธีที่เหมาะสมที่สุดในการบรรเทาความเสี่ยงที่มีโอกาสเกิดน้อย แต่ผลกระทบสูง
    1. avoid the risk 2. accept the risk
    3. transfer the risk 4. mitigate the risk
    5. change the risk

Concept & Protection in Network (Case Study)

• root.exe?/c+dir in which environment
    Choices: Windows/Linux + IIS/Apache
• Class ไหนมี host 254 เครื่อง

Choices: a, b, c, d

- ข้อใดเป็นการโจมตีที่ไม่ใช่ application layer : slowloris,ping
- IPv6 มีกี่ address 3.4 * 10^38
- IPv6 advantage over [2^128] ipv4
- Block SMB port? TCP/UDP? 135,136,137,445?

Concept & Protection in Data Center (Case Study)

- แมลงที่มีผลต่อ datacenter

  Choices: แมงสาบ, แมงมุม, มด,?
- Datacenter backup site characteristic
- ข้อใดต้องคำนึงน้อยที่สุดสำหรับ data center,ห้องควบคุม

  Choices: ความชื้น, อุณหภูมิ, กระแสไฟฟ้า,?
- ข้อใดไม่ควรทำกับ data center

  Choices: บนพื้น raise floor 20m,

กำแพงกระจกหันหน้าเข้าแดดเพื่อระบายความชื้น, พื้น

Concept & Protection in Malicious war (Case Study)

- apt ย่อมาจาก advanced persistent threat

Concept & Protection Computer Fraud (Case Study)

- computer fraud ส่วนมากเกิดจาก
- choices: man-in-the-browser
- fraud เกิดจาก การเงิน กดดันการทำงาน

Concept & Protection in Application (Case Study)

• buff[6] string = "1234556678" strcpy(buff, string) overflow แบบใด heap, stack
• มาตรฐานซอฟต์แวร์ CMMI

Concept & Protection Physical environment (Case Study)

• fm200, h2o effect
    Choices: fiber optic พัง, คอมพัง, คนตาย
• Backup Site อยู่ห่างกี่กม.
• backup link between branch

Concept of Incident Response & Business Continuity (Case Study)

• Business continuity plan

Concept of Security on Mobile, Cloud Computing and Social Media (Case Study)

• Amazon EC2 … (something) …