วัตถุประสงค์ของ
การสอบประกาศนียบัตร
CompTIA PenTest+

รหัสข้อสอบ: **PT0-002**

เกี่ยวกับข้อสอบ

ผู้สมัครสอบสามารถใช้เอกสารฉบับนี้เพื่อช่วยเตรียมความพร้อมสำหรับการสอบประกาศนียบัตร CompTIA PenTest+ (PT0-002) การสอบประกาศนียบัตร CompTIA PenTest+ จะรับรองว่าผู้สมัครซึ่งสอบผ่านมีความรู้และทักษะที่จำเป็นในการ:

- **วางแผนและกำหนดขอบเขตข้อตกลงการทดสอบเจาะระบบ**
- **เข้าใจข้อกำหนดทางกฎหมายและการปฏิบัติตามข้อบังคับ**
- **ดำเนินการสแกนหาช่องโหว่และการทดสอบเจาะระบบโดยใช้เครื่องมือและเทคนิคที่เหมาะสม จากนั้นวิเคราะห์ผลลัพธ์**
- **จัดทำรายงานเป็นลายลักษณ์อักษรซึ่งประกอบด้วยเทคนิคการแก้ไขที่นำเสนอ สื่อสารผลลัพธ์ไปยังทีมผู้บริหารอย่างมีประสิทธิภาพ และให้คำแนะนำที่ปฏิบัติได้จริง**

ข้อสอบนี้เทียบเท่ากับประสบการณ์การทำงานจริงสามถึงสี่ปีในบทบาทหน้าที่ของที่ปรึกษาด้านความปลอดภัยหรือผู้ทดสอบเจาะระบบ

ตัวอย่างเนื้อหาเหล่านี้ให้ไว้เพื่ออธิบายวัตถุประสงค์เท่านั้น ไม่ใช่รายการหัวข้อเนื้อหาทั้งหมดของข้อสอบชุดนี้

การรับรองการสอบ

ข้อสอบ CompTIA PenTest+ (PT0-002) ผ่านการรับรองจากสถาบันมาตรฐานอเมริกัน (ANSI) ตามมาตรฐาน ISO 17024 ซึ่งผ่านการทบทวนและปรับปรุงวัตถุประสงค์ของข้อสอบอย่างสม่ำเสมอ

การพัฒนาข้อสอบ

ข้อสอบ CompTIA เป็นผลจากการประชุมเชิงปฏิบัติการของผู้เชี่ยวชาญในหัวข้อเนื้อหาที่สำคัญ และผลสำรวจเกี่ยวกับทักษะและความรู้ที่จำเป็นสำหรับผู้ประกอบวิชาชีพด้าน IT ระดับผู้เชี่ยวชาญในอุตสาหกรรม

นโยบายการใช้เนื้อหาที่ได้รับอนุญาตของ CompTIA

CompTIA Certifications, LLC ไม่มีส่วนเกี่ยวข้องกับและไม่ได้อนุญาต สนับสนุน หรือยอมให้มีการใช้เนื้อหาใดที่จัดหาให้โดยเว็บไซต์การฝึกอบรมภายนอกที่ไม่ได้รับอนุญาต (หรือที่เรียกว่า “Brain dumps”) ผู้ที่ใช้เนื้อหาดังกล่าวเพื่อเตรียมความพร้อมสำหรับการสอบ CompTIA ใด ๆ จะถูกเพิกถอนประกาศนียบัตรของตนและระงับการทดสอบในอนาคต ตามข้อตกลงผู้สมัครสอบ CompTIA ด้วยความพยายามที่จะสื่อสารนโยบายการสอบว่าด้วยเนื้อหาการเรียนรู้ที่ไม่ได้รับอนุญาตของ CompTIA ให้ชัดเจนยิ่งขึ้น CompTIA จึงแนะนำให้ผู้สมัครสอบประกาศนียบัตรทุกท่านไปที่**นโยบายการสอบประกาศนียบัตร CompTIA** โปรดทบทวนนโยบายทั้งหมดของ CompTIA ก่อนที่จะเริ่มต้นกระบวนการเรียนรู้สำหรับการสอบ CompTIA ใด ๆ ผู้สมัครสอบจะต้องปฏิบัติตาม**ข้อตกลงผู้สมัครสอบ CompTIA** หากผู้สมัครสอบมีคำถามเกี่ยวกับเนื้อหาการเรียนรู้ที่ถือว่าไม่ได้รับอนุญาต (หรือที่เรียกว่า “brain dumps”) ผู้สมัครสอบควรติดต่อ CompTIA ที่ **examsecurity@comptia.org** เพื่อตรวจสอบยืนยัน

โปรดทราบ

รายการตัวอย่างที่ให้ไว้ในสัญลักษณ์แสดงหัวข้อย่อยเป็นเพียงรายการคร่าว ๆ ตัวอย่างเทคโนโลยี กระบวนการ หรืองานอื่นที่สัมพันธ์กับวัตถุประสงค์แต่ละข้ออาจรวมอยู่ในข้อสอบ แม้ว่าจะไม่ได้อยู่ในรายการหรือถูกกล่าวถึงในเอกสารวัตถุประสงค์ฉบับนี้ก็ตาม CompTIA ได้ทำการทบทวนเนื้อหาข้อสอบและปรับปรุงคำถามในข้อสอบอย่างต่อเนื่อง เพื่อให้ข้อสอบของเราเป็นปัจจุบันและเพื่อรักษาความปลอดภัยในการเก็บรักษาคำถามให้เป็นความลับ ในกรณีที่จำเป็น เราจะจัดทำข้อสอบฉบับปรับปรุงโดยอ้างอิงจากจุดประสงค์ของข้อสอบเดิม โปรดทราบว่าสื่อเตรียมสอบทั้งหมดที่เกี่ยวข้องจะยังคงสามารถใช้ได้อยู่

รายละเอียดการทดสอบ

ข้อสอบที่จำเป็น	PT0-002
จำนวนคำถาม	สูงสุด 85 ข้อ
ประเภทคำถาม	ข้อสอบแบบเลือกตอบและอ้างอิงตามผลการดำเนินงาน
ระยะเวลาการทดสอบ	165 นาที
ประสบการณ์ที่แนะนำ	ประสบการณ์ตรง 3–4 ปีในการปฏิบัติหน้าที่ ทดสอบเจาะระบบ ประเมินช่องโหว่ และวิเคราะห์โค้ด
คะแนนที่ให้ผ่าน	750 (ในระดับคะแนน 100-900)

วัตถุประสงค์การสอบ (ขอบเขต)

ตารางด้านล่างแสดงขอบเขตการวัดผลของข้อสอบชุดนี้และสัดส่วนการให้คะแนน

ขอบเขต	อัตราส่วนร้อยละของข้อสอบ
1.0 การวางแผนและการกำหนดขอบเขต	14%
2.0 การรวบรวมข้อมูลและการสแกนช่องโหว่	22%
3.0 การโจมตีและการหาประโยชน์จากช่องโหว่	30%
4.0 การรายงานและการสื่อสาร	18%
5.0 เครื่องมือและการวิเคราะห์โค้ด	16%
รวม	**100%**

1.0 การวางแผนและการกำหนดขอบเขต

1.1 เปรียบเทียบและแสดงข้อแตกต่างของแนวคิดการกำกับดูแล ความเสี่ยง และการปฏิบัติตามข้อบังคับ

- **ข้อควรพิจารณาด้านการปฏิบัติตามข้อบังคับ**
  - Payment Card Industry Data Security Standard (PCI DSS)
  - General Data Protection Regulation (GDPR)
- **ข้อจำกัดด้านตำแหน่งที่ตั้ง**
  - ข้อจำกัดของประเทศ
  - ข้อจำกัดของเครื่องมือ
  - กฎหมายท้องถิ่น
  - ข้อกำหนดของรัฐบาลท้องถิ่น
  - ข้อกำหนดความเป็นส่วนตัว
- **แนวคิดทางกฎหมาย**
  - สัญญาระดับการบริการ (SLA)
  - การเก็บรักษาความลับ
  - คำชี้แจงการทำงาน
  - ข้อตกลงไม่เปิดเผย (NDA)
  - สัญญาการให้บริการหลัก
- **การอนุญาตให้โจมตี**

1.2 อธิบายความสำคัญของการกำหนดขอบเขตและข้อกำหนดขององค์กร/ลูกค้า

- **มาตรฐานและระเบียบวิธี**
  - MITRE ATT&CK
  - Open Web Application Security Project (OWASP)
  - National Institute of Standards and Technology (NIST)
  - Open-source Security Testing Methodology Manual (OSSTMM)
  - Penetration Testing Execution Standard (PTES)
  - Information Systems Security Assessment Framework (ISSAF)
- **กฎการปะทะ**
  - เวลาของวัน
  - ประเภทของการทดสอบที่อนุญาต/ไม่อนุญาต
  - ข้อจำกัดอื่น ๆ
- **ข้อควรพิจารณาด้านสภาพแวดล้อม**
  - เครือข่าย
  - แอปพลิเคชัน
  - ระบบคลาวด์
- **รายการเป้าหมาย/สินทรัพย์ในขอบเขต**
  - เครือข่ายไร้สาย
  - ช่วงของอินเทอร์เน็ตโปรโตคอล (IP)
  - โดเมน
  - ส่วนต่อประสานโปรแกรม ประยุกต์ (API)
  - ตำแหน่งทางกายภาพ
  - ระบบโดเมนเนม (DNS)
  - เป้าหมายภายนอกกับภายใน
  - บุคคลที่หนึ่งกับบุคคลที่สามที่โฮสต์
- **ตรวจสอบขอบเขตของการว่าจ้าง**
  - สอบถามลูกค้า/ตรวจสอบสัญญา
  - การบริหารเวลา
  - กลยุทธ์
    - การทดสอบที่ไม่ทราบสภาพแวดล้อมกับที่ทราบสภาพแวดล้อม

1.3 จากสถานการณ์ที่กำหนด แสดงให้เห็นถึงกรอบความคิดในการแฮกข้อมูลอย่างมีจริยธรรม โดยคงไว้ซึ่งความเป็นมืออาชีพและความซื่อสัตย์

- **ตรวจสอบประวัติของ ทีมทดสอบเจาะระบบ**
- **ยึดตามขอบเขตเฉพาะของการว่าจ้าง**
- **ระบุกิจกรรมที่เป็นอาชญากรรม**
- **รายงานการฝ่าฝืน/กิจกรรมที่เป็นอาชญากรรมโดยทันที**
- **จำกัดการใช้เครื่องมือไว้ที่ การว่าจ้างซึ่งจำเพาะเจาะจง**
- **จำกัดการรุกล้ำให้เป็นไปตามขอบเขต**
- **รักษาความลับของข้อมูล /สารสนเทศ**
- **ความเสี่ยงต่อผู้เชี่ยวชาญในวิชาชีพ**
  - ค่าธรรมเนียม/ค่าปรับ
  - ความผิดทางอาญา

2.0 การรวบรวมข้อมูล และการสแกนช่องโหว่

2.1 จากสถานการณ์ที่กำหนด ให้ทำการสอดส่องแบบเชิงรับ

- **การค้นหา DNS**
- **ระบุข้อมูลติดต่อด้านเทคนิค**
- **ข้อมูลติดต่อผู้ดูแลระบบ**
- **ระบบคลาวด์กับการโฮสต์เอง**
- **การดึงข้อมูลโซเชียลมีเดีย**
  - ข้อมูลติดต่อสำคัญ/หน้าที่รับผิดชอบในงาน
  - การรับสมัครงาน/เทคโนโลยีที่ใช้
- **ข้อบกพร่องของการเข้ารหัส**
  - ใบรับรอง Secure Sockets Layer (SSL)
  - การเพิกถอน
- **ชื่อเสียงของบริษัท/การรักษาความปลอดภัย**
- **ข้อมูล**
  - การถ่ายโอน (dump) รหัสผ่าน
  - ไฟล์เมตาดาต้า
  - การวิเคราะห์เครื่องมือค้นหา เชิงกลยุทธ์/การระบุแจกแจง
  - เว็บไซต์ที่เก็บถาวร/การแคช
  - ที่เก็บซอร์สโค้ดสาธารณะ
- **ข่าวกรองแบบโอเพ่นซอร์ส (OSINT)**
  - เครื่องมือ
    - Shodan
    - Recon-ng
  - แหล่งที่มา
    - Common weakness enumeration (CWE)
    - Common vulnerabilities and exposures (CVE)

2.2 จากสถานการณ์ที่กำหนด ให้ทำการสอดส่องแบบเชิงรุก

- **การระบุแจกแจง**
  - โฮสต์
  - บริการ
  - โดเมน
  - ผู้ใช้
  - ตัวระบุตำแหน่งในอินเทอร์เน็ต (URL)
- **การสอดส่องเว็บไซต์**
  - การรวบรวมข้อมูลเว็บไซต์
  - การดึงข้อมูลเว็บไซต์
  - การตรวจสอบเว็บลิงก์ด้วยตนเอง
    - robots.txt
- **การสร้างแพ็กเก็ต (Packet crafting)**
  - Scapy
- **การตรวจจับการป้องกัน**
  - การตรวจจับเครื่องกระจายโหลด
  - การตรวจจับไฟร์วอลล์เว็บแอปพลิเคชัน (WAF)
  - โปรแกรมป้องกันไวรัส
  - ไฟร์วอลล์
- **โทเค็น**
  - การกำหนดขอบเขต
  - การออก
  - การเพิกถอน
- **วอร์ไดรฟ์วิ่ง (Wardriving)**
- **ทราฟฟิกของเครือข่าย**
  - ดักจับคำขอและการตอบกลับของ API
  - การดักจับข้อมูล (Sniffing)
- **การค้นพบสินทรัพย์บนคลาวด์**
- **บริการโฮสต์โดยบุคคลที่สาม**
- **การหลีกเลี่ยงการตรวจจับ**

2.3 จากสถานการณ์ที่กำหนด ให้วิเคราะห์ผลของการปฏิบัติการสอดส่อง

- **การระบุอัตลักษณ์ (Fingerprinting)**
  - ระบบปฏิบัติการ (OS)
  - เครือข่าย
  - อุปกรณ์เครือข่าย
  - ซอฟต์แวร์
- **วิเคราะห์เอาต์พุตจาก:**
  - การค้นหา DNS
  - การรวบรวมข้อมูลเว็บไซต์
  - ทราฟฟิกของเครือข่าย
  - ทราฟฟิก Address Resolution Protocol (ARP)
  - สแกน Nmap
  - บันทึก (logs) ของเว็บ

2.4 จากสถานการณ์ที่กำหนด ให้ดำเนินการสแกนช่องโหว่

- **ข้อควรพิจารณาในการสแกนช่องโหว่**
  - เวลาที่รันการสแกน
  - โปรโตคอล
  - แผนผังของเครือข่าย
  - ข้อจำกัดแบนด์วิดท์
  - การควบคุมปริมาณ Query
  - ระบบที่เปราะบาง
  - สินทรัพย์ที่ไม่ใช่แบบซึ่งใช้กันทั่วไป
- **สแกนเป้าหมายที่ระบุเพื่อหาช่องโหว่**
- **ตั้งค่าการสแกนเพื่อหลีกเลี่ยงการตรวจจับ**
- **วิธีการสแกน**
  - การลักลอบสแกน
  - การสแกนโดยเชื่อมต่อด้วย Transmission Control Protocol (TCP)
  - มีข้อมูลสิทธิ์เข้าระบบและไม่มีข้อมูลสิทธิ์เข้าระบบ
- **Nmap**
  - สคริปต์ Nmap Scripting Engine (NSE)
  - ตัวเลือกทั่วไป
    - -A
    - -sV
    - -sT
    - -Pn
    - -O
    - -sU
    - -sS
    - -T 1-5
    - -script=vuln
    - -p
- **เครื่องมือทดสอบช่องโหว่ที่ สามารถกำหนดให้ทำอัตโนมัติ**

3.0 การโจมตีและการหาประโยชน์จากช่องโหว่

3.1 จากสถานการณ์ที่กำหนด ให้ค้นคว้าเกี่ยวกับเวกเตอร์โจมตีและทำการโจมตีเครือข่าย

- **การทดสอบความเครียดเพื่อความพร้อมใช้งาน**
- **ใช้ประโยชน์จากทรัพยากร**
  - ใช้ประโยชน์จากฐานข้อมูล (DB)
  - พายุแพ็กเก็ต (Packet storm)
- **โจมตี**
  - การปลอมแปลง ARP
  - ห่วงโซ่การหาประโยชน์
  - การโจมตีรหัสผ่าน
    - การโจมตีหลายบัญชีด้วยรหัสผ่านที่คนมักใช้
    - การถอดรหัส Hash
    - การสุ่มรหัสผ่าน (Brute force)
    - การสุ่มรหัสผ่านจากพจนานุกรม
  - การถูกแทรกแซงโดยผู้ไม่หวังดี (On-path/man-in-the-middle)
  - การโจมตี Kerberos (Kerberoasting)
  - การปลอมแปลงแคช DNS
  - การกระโดดข้ามเครือข่ายท้องถิ่นแบบเสมือน (VLAN hopping)
  - การบายพาสการควบคุมการเข้าถึงเครือข่าย (NAC)
  - การปลอมแปลง MAC Address
  - การปลอมแปลง Link-Local Multicast Name Resolution (LLMNR)/ NetBIOS-Name Service (NBT-NS)
  - การโจมตี New Technology LAN Manager (NTLM) relay
- **เครื่องมือ**
  - Metasploit
  - Netcat
  - Nmap

3.2 จากสถานการณ์ที่กำหนด ให้ค้นคว้าเกี่ยวกับเวกเตอร์โจมตีและทำการโจมตีแบบไร้สาย

- **วิธีการโจมตี**
  - การลอบฟัง
  - การปรับเปลี่ยนข้อมูล
  - ทำให้ข้อมูลเสียหาย
  - การโจมตีแบบรีเลย์
  - การปลอมตัว
  - ปฏิเสธการพิสูจน์ตัวตน (Deauthentication)
  - รบกวนสัญญาณ
  - ดักจับ Handshake
  - การถูกแทรกแซงโดยผู้ไม่หวังดี (On-path)
- **โจมตี**
  - การปล่อยสัญญาณปลอม (Evil twin)
  - พอร์ทัลคัดกรอง
  - การส่งข้อมูลผ่านทางบลูทูธ (Bluejacking)
  - การเชื่อมต่อโดยไม่ได้รับอนุญาตผ่านทางบลูทูธ (Bluesnarfing)
  - การโคลนการระบุความถี่ วิทยุ (RFID)
  - การโจมตี Bluetooth Low Energy (BLE)
  - การโจมตีแบบ Amplification [Near Field Communication (NFC)]
  - การโจมตี PIN ของการตั้งค่าแบบ WiFi Protected Setup (WPS)
- **เครื่องมือ**
  - Aircrack-ng Suite
  - เสาอากาศขยายเกณฑ์

3.3 จากสถานการณ์ที่กำหนด ให้ค้นคว้าเกี่ยวกับเวกเตอร์โจมตีและทำการโจมตีแบบตามแอปพลิเคชัน

- **OWASP 10 อันดับ**
- **การปลอมคำขอฝั่งเซิร์ฟเวอร์**
- **ข้อบกพร่องของตรรกะธุรกิจ**
- **การโจมตีด้วยการ Injection**
  - Structured Query Language (SQL) injection
    - Blind SQL
    - Boolean SQL
    - Stacked queries
  - Command injection
  - Cross-site scripting
    - Persistent
    - Reflected
  - Lightweight Directory Access Protocol (LDAP) injection
- **ช่องโหว่ของแอปพลิเคชัน**
  - Race conditions
  - ขาดการจัดการข้อผิดพลาด
  - ขาดการเข็นกำกับโค้ด
  - การส่งข้อมูลที่ไม่ปลอดภัย
  - การโจมตีเซสชัน
    - Session hijacking
    - การปลอมแปลงคำขอข้ามไซต์ (CSRF)
    - การยกระดับสิทธิ์
    - การทำซ้ำเซสชัน
    - การสวมสิทธิ์เซสชัน
- **การโจมตี API**
  - Restful
  - Extensible Markup Language-Remote Procedure Call (XML-RPC)
  - Soap
- **การเข้าถึงผ่านไดเรกทอรี (directory traversal)**
- **เครื่องมือ**
  - พร็อกซี่เว็บ
    - OWASP Zed Attack Proxy (ZAP)
    - Burp Suite รุ่นชุมชน
  - SQLmap
  - DirBuster
- **ทรัพยากร**
  - รายการคำ

3.4 จากสถานการณ์ที่กำหนด ให้ค้นคว้าเกี่ยวกับเวกเตอร์โจมตีและทำการโจมตีบนเทคโนโลยีคลาวด์

- **โจมตี**
  - การรวบรวมข้อมูลประจำตัว
  - การยกระดับสิทธิ์
  - การยึดครองบัญชี
  - การโจมตีบริการเมตาดาต้า
  - สินทรัพย์คลาวด์ที่กำหนดค่าไม่ถูกต้อง
    - การจัดการข้อมูลประจำตัว และการเข้าถึง (IAM)
    - การกำหนดค่า Federation ไม่ถูกต้อง
    - การจัดเก็บวัตถุ
    - เทคโนโลยีการรันในคอนเทนเนอร์
  - การใช้ทรัพยากรหมดไป
  - การโจมตีด้วยการฉีดมัลแวร์คลาวด์
  - การโจมตีแบบปฏิเสธการให้บริการ
  - การโจมตีแบบ Side-channel
  - การโจมตีโดยตรงไปยังต้นทาง
- **เครื่องมือ**
  - Software Development Kit (SDK)

3.5 อธิบายการโจมตีทั่วไปและช่องโหว่ของระบบเฉพาะทาง

- **มือถือ**
  - โจมตี
    - วิศวกรรมย้อนกลับ
    - การวิเคราะห์แซนด์บ็อกซ์
    - การสแปม
  - ช่องโหว่
    - การจัดเก็บที่ไม่ปลอดภัย
    - ช่องโหว่ของรหัสผ่าน
    - การปักหมุดใบรับรอง
    - การใช้ส่วนประกอบที่มีช่องโหว่ที่รู้จัก
      - (i) ช่องโหว่ของการพึ่งพา
      - (ii) การแก้ไขการกระจายตัว
    - การดำเนินกิจกรรมโดยใช้รูท
    - เกินสิทธิ์ที่อนุญาต
    - การรวมชีวมาตร
    - ช่องโหว่ของตรรกะธุรกิจ
  - เครื่องมือ
    - Burp Suite
    - Drozer
    - Mobile Security Framework (MobSF)
    - Postman
    - Ettercap
    - Frida
    - Objection
    - เครื่องมือ Android SDK
    - ApkX
    - APK Studio
- **อุปกรณ์อินเทอร์เน็ตของสรรพสิ่ง (IoT)**
  - การโจมตี BLE
  - การพิจารณาเป็นพิเศษ
    - สภาพแวดล้อมที่เปราะบาง
    - ข้อกังวลด้านความพร้อมใช้งาน
    - ข้อมูลเสียหาย
    - การแอบดึงข้อมูล
  - ช่องโหว่
    - ค่าเริ่มต้นที่ไม่ปลอดภัย
    - การสื่อสารด้วยข้อความปกติที่ไม่เข้ารหัส
    - การกำหนดค่าฮาร์ดโค้ด
    - เฟิร์มแวร์/ฮาร์ดแวร์ที่ล้าสมัย
    - ข้อมูลรั่วไหล
    - การใช้ส่วนประกอบที่ไม่ปลอดภัยหรือล้าสมัย
- **ช่องโหว่ของระบบจัดเก็บข้อมูล**
  - การกำหนดค่าผิดพลาดในองค์กรและบนคลาวด์
    - ค่าเริ่มต้น/ค่าว่างชื่อผู้ใช้/รหัสผ่าน
    - การเปิดเผยเครือข่าย
  - ขาดการล้างข้อมูลอินพุตผู้ใช้
  - ช่องโหว่ของซอฟต์แวร์พื้นฐาน
    - ข้อความแสดงข้อผิดพลาดและการจัดการแก้จุดบกพร่อง
    - ช่องโหว่ของ Injection
      - วิธีแบบ Single quote
- **ช่องโหว่ของอินเทอร์เฟซการจัดการ**
  - Intelligent platform management interface (IPMI)
- **ช่องโหว่ที่เกี่ยวข้องกับ supervisory control and data acquisition (SCADA)/ Industrial Internet of Things (IIoT)/ industrial control system (ICS)**
- **ช่องโหว่ที่เกี่ยวข้องกับสภาพแวดล้อมเสมือน**
  - การหลบหนี Virtual machine (VM)
  - ช่องโหว่ของไฮเปอร์ไวเซอร์
  - ช่องโหว่ของคลังเก็บ VM
- **ช่องโหว่ที่เกี่ยวข้องกับปริมาณงานที่รันในคอนเทนเนอร์**

3.6 จากสถานการณ์ที่กำหนด ให้ทำการโจมตีแบบวิศวกรรมสังคมหรือแบบกายภาพ

- **การแอบอ้างเพื่อการเข้าถึง**
- **การโจมตีด้วยวิศวกรรมสังคม**
  - อีเมลฟิชชิง
    - เวลลิง (Whaling)
    - สเปียร์ฟิชชิง (Spear phishing)
  - วิชชิง (Vishing)
  - ฟิชชิงบริการข้อความสั้น (SMS)
  - การปล่อย Universal Serial Bus (USB) key
  - การโจมตีแบบ Watering hole
- **การโจมตีทางกายภาพ**
  - การลักลอบเข้าบริเวณต้องจำกัดโดยไม่ได้รับอนุญาต (Tailgating)
  - การค้นข้อมูลจากถังขยะ
  - การแอบดูข้อมูลโดยยืนข้างหลังมองข้ามไหล่ (Shoulder surfing)
  - การโคลนป้ายชื่อ
- **การปลอมตัวเป็นผู้อื่น (impersonation)**
- **เครื่องมือ**
  - Browser exploitation framework (BeEF)
  - ชุดเครื่องมือวิศวกรรมสังคม
  - เครื่องมือปลอมแปลงการโทร
- **วิธีของการโน้มน้าว**
  - อำนาจหน้าที่
  - ความขาดแคลน
  - ข้อพิสูจน์ทางสังคม
  - ความเร่งด่วน
  - ความคล้ายคลึง
  - ความกลัว

3.7 จากสถานการณ์ที่กำหนด ให้ใช้เทคนิคหลังการหาประโยชน์

- **เครื่องมือหลังการหาประโยชน์**
  - Empire
  - Mimikatz
  - BloodHound
- **การเคลื่อนย้ายตัวเอง (Lateral movement)**
  - การใช้รหัสผ่านที่ถูกแฮชไว้โดยไม่ต้องแกะรหัสแฮช (Pass the hash)
- **การทดสอบการแบ่งส่วนเครือข่าย**
- **การยกระดับสิทธิ์ (privilege escalation)**
  - แนวนอน (Horizontal)
  - แนวตั้ง (Vertical)
- **การอัปเกรดเชลล์ที่มีข้อจำกัด**
- **การสร้างฐานที่มั่นคง/ความทนทาน**
  - โทรจัน
  - Backdoor
    - Bind shell
    - Reverse shell
  - Daemons
  - งานที่กำหนดเวลาไว้
- **การหลีกเลี่ยงการตรวจจับ**
  - เทคนิค Living-off-the-land /มัลแวร์ที่ไม่มีไฟล์
    - PsExec
    - Windows Management Instrumentation (WMI)
    - การรีโมท PowerShell (PS)/Windows Remote Management (WinRM)
  - การแอบดึงข้อมูล
  - การปกปิดร่องรอยของคุณ
  - การอำพรางข้อมูล (Steganography)
  - การสร้างช่องทางลับ
- **การระบุแจกแจง**
  - ผู้ใช้
  - กลุ่ม
  - ฟอเรสต์
  - ข้อมูลที่มีความอ่อนไหว
  - ไฟล์ที่ไม่ได้เข้ารหัส

4.0 การรายงานและการสื่อสาร

4.1 เปรียบเทียบและแสดงข้อแตกต่างขององค์ประกอบที่สำคัญของรายงานที่เป็นลายลักษณ์อักษร

- **ผู้ฟังรายงาน**
  - C-suite
  - บุคคลที่สามผู้มีส่วนได้ส่วนเสีย
  - เจ้าหน้าที่ทางเทคนิค
  - นักพัฒนา
- **เนื้อหารายงาน (** ไม่ได้เรียงลำดับเฉพาะ)**
  - บทสรุปการดำเนินการ
  - รายละเอียดขอบเขต
  - ระเบียบวิธี
    - การบรรยายการโจมตี
  - สิ่งที่พบ
    - ระดับความเสี่ยง (กรอบงานอ้างอิง)
    - การจัดลำดับความเสี่ยง
    - การวิเคราะห์ผลกระทบทางธุรกิจ
  - ตัวชี้วัดและมาตรการ
  - การแก้ไข
  - ข้อสรุป
  - ภาคผนวก
- **เวลาในการจัดเก็บรายงาน**
- **การแจกจ่ายที่ปลอดภัย**
- **การจดบันทึก**
  - เอกสารต่อเนื่องระหว่างการทดสอบ
  - ภาพหน้าจอ
- **ประเด็นทั่วไป/สาเหตุหลัก**
  - ช่องโหว่
  - ข้อสังเกต
  - การขาดแนวปฏิบัติที่ดี

4.2 จากสถานการณ์ที่กำหนด ให้วิเคราะห์สิ่งที่ค้นพบและแนะนำการแก้ไขที่เหมาะสมในรายงาน

- **การควบคุมเชิงเทคนิค**
  - การเสริมความปลอดภัยของระบบ
  - ล้างข้อมูลอินพุตผู้ใช้/แบบสอบถามที่กำหนดค่าพารามิเตอร์
  - ใช้การพิสูจน์ตัวตนแบบ หลายปัจจัย
  - เข้ารหัสรหัสผ่าน
  - การแก้ไขระดับกระบวนการ
  - การจัดการแพทช์
  - การหมุนเวียนเปลี่ยน Key
  - การจัดการใบรับรอง
  - โซลูชันการจัดการความลับ
  - การแบ่งส่วนเครือข่าย
- **การควบคุมดูแลระบบ**
  - การควบคุมการเข้าถึงตามบทบาทหน้าที่
  - วงจรของการพัฒนาซอฟต์แวร์ที่ปลอดภัย
  - ข้อกำหนดรหัสผ่านขั้นต่ำ
  - นโยบายและขั้นตอน
- **การควบคุมการปฏิบัติงาน**
  - การหมุนเวียนเปลี่ยนงาน
  - การจำกัดการใช้งานในบางช่วงเวลาของวัน
  - การบังคับลาพักร้อน
  - การฝึกอบรมผู้ใช้
- **การควบคุมทางกายภาพ**
  - ห้องโถงที่มีการควบคุมการเข้าถึง
  - การควบคุมทางชีวมาตร
  - การสังเกตการณ์ด้วยกล้องวิดีโอ

4.3 อธิบายความสำคัญของการสื่อสารระหว่างขั้นตอนการทดสอบเจาะระบบ

- **เส้นทางการสื่อสาร**
  - ผู้ติดต่อหลัก
  - ผู้ติดต่อด้านเทคนิค
  - ผู้ติดต่อกรณีฉุกเฉิน
- **สิ่งกระตุ้นการสื่อสาร**
  - การค้นพบที่สำคัญ
  - รายงานสถานะ
  - สัญญาณบ่งชี้ของการละเมิดก่อนหน้านี้
- **เหตุผลในการสื่อสาร**
  - การรับรู้สถานการณ์
  - การลดระดับ
  - การไม่ขัดแย้ง
  - การระบุผลบวกลวง
  - กิจกรรมที่เป็นอาชญากรรม
- **การจัดลำดับความสำคัญของเป้าหมายใหม่**
- **การนำเสนอสิ่งที่ค้นพบ**

4.4 อธิบายกิจกรรมหลังการส่งรายงาน

- **การชำระล้างหลังการทดสอบ**
  - การลบเซลล์
  - การลบข้อมูลประจำตัวที่สร้างโดยผู้ทดสอบ
  - การลบเครื่องมือ
- **การยอมรับของลูกค้า**
- **การเรียนรู้บทเรียน**
- **การติดตามผล/ทดสอบซ้ำ**
- **การรับรองสิ่งที่ค้นพบ**
- **กระบวนการทำลายข้อมูล**

5.0 เครื่องมือและการวิเคราะห์โค้ด

5.1 อธิบายแนวคิดพื้นฐานของการเขียนสคริปต์และการพัฒนาซอฟต์แวร์

- **โครงสร้างตรรกะ**
  - ลูป (Loop)
  - เงื่อนไข
  - ตัวดำเนินการ Boolean
  - ตัวดำเนินการ String
  - ตัวดำเนินการคณิตศาสตร์
- **โครงสร้างข้อมูล**
  - JavaScript Object Notation (JSON)
  - Key value
  - Arrays
  - พจนานุกรม
  - Comma-Separated Value (CSV)
  - รายการ
  - ทรี (Tree)
- **ไลบรารี (Library)**
- **คลาส (Classe)**
- **ขั้นตอน**
- **ฟังก์ชัน**

5.2 จากสถานการณ์ที่กำหนด ให้วิเคราะห์ตัวอย่างสคริปต์หรือโค้ดเพื่อใช้ในการทดสอบเจาะระบบ

- **เชลล์ (Shell)**
  - Bash
  - PS
- **ภาษาการเขียนโปรแกรม**
  - Python
  - Ruby
  - Perl
  - JavaScript
- **วิเคราะห์รหัสการเจาะระบบเพื่อ:**
  - ดาวน์โหลดไฟล์
  - เปิดการเข้าถึงระยะไกล
  - แจกแจงผู้ใช้
  - แจกแจงทรัพย์สิน
- **โอกาสสำหรับระบบอัตโนมัติ**
  - กระบวนการทดสอบเจาะระบบอัตโนมัติ
    - ทำการสแกนพอร์ต จากนั้นดำเนินการขั้นต่อไปโดยอัตโนมัติตามผลลัพธ์
    - ตรวจสอบการกำหนดค่า และจัดทำรายงาน
  - การเขียนสคริปต์เพื่อแก้ไข IP address ระหว่างการทดสอบ
  - การเขียนสคริปต์ Nmap เพื่อแจกแจง รหัสและจัดทำรายงาน

5.3 อธิบายกรณีการใช้งานของเครื่องมือดังต่อไปนี้ในระหว่างขั้นตอนของการทดสอบเจาะระบบ

*(**เจตนาของวัตถุประสงค์นี้ไม่ใช่เพื่อทดสอบชุดคุณสมบัติของผู้จำหน่ายที่เฉพาะเจาะจง)*

- **เครื่องสแกน**
  - Nikto
  - Open Vulnerability Assessment Scanner (Open VAS)
  - SQLmap
  - Nessus
  - Open Security Content Automation Protocol (SCAP)
  - Wapiti
  - WPScan
  - Brakeman
  - Scout Suite
- **เครื่องมือทดสอบข้อมูลประจำตัว**
  - Hashcat
  - Medusa
  - Hydra
  - CeWL
  - John the Ripper
  - Cain
  - Mimikatz
  - Patator
  - DirBuster
- **เครื่องมือแก้จุดบกพร่อง**
  - OllyDbg
  - Immunity Debugger
  - GNU Debugger (GDB)
  - WinDbg
  - Interactive Disassembler (IDA)
  - Covenant
  - SearchSploit
- **OSINT**
  - WHOIS
  - Nslookup
  - Fingerprinting Organization with Collected Archives (FOCA)
  - theHarvester
  - Shodan
  - Maltego
  - Recon-ng
  - Censys
- **แบบไร้สาย**
  - ชุด Aircrack-ng
  - Kismet
  - Wifite2
  - อุปกรณ์กระจายสัญญาณหลอกลวง
  - EAPHammer
  - mdk4
  - Spooftooph
  - Reaver
  - Wireless Geographic Logging Engine (WiGLE)
  - Fern
- **เครื่องมือเว็บแอปพลิเคชัน**
  - OWASP ZAP
  - Burp Suite
  - Gobuster
  - w3af
- **เครื่องมือวิศวกรรมสังคม**
  - ชุดเครื่องมือวิศวกรรมสังคม (SET)
  - BeEF
- **เครื่องมือการเข้าถึงระยะไกล**
  - Secure Shell (SSH)
  - Ncat
  - Netcat
  - ProxyChains
- **เครื่องมือเครือข่าย**
  - Wireshark
  - Hping
- **อื่นๆ**
  - SearchSploit
  - ตัวตอบสนอง
  - เครื่องมือ Impacket
  - Empire
  - Metasploit
  - mitm6
  - CrackMapExec
  - TruffleHog
  - Censys
- **เครื่องมืออำพรางข้อมูล**
  - Openstego
  - Steghide
  - Snow
  - Coagula
  - Sonic Visualiser
  - TinEye
- **เครื่องมือคลาวด์**
  - Scout Suite
  - CloudBrute
  - Pacu
  - Cloud Custodian

รายการคำย่อของ PenTest+ (PT0-002)

รายการต่อไปนี้คืออักษรย่อที่ปรากฏในข้อสอบ CompTIA PenTest+ ผู้สมัครสอบควรทบทวนรายการทั้งหมดและศึกษาหาความรู้ในการปฏิบัติงานเกี่ยวกับอักษรย่อทั้งหมดเพื่อการเตรียมความพร้อมสำหรับการสอบที่ครอบคลุม

คำย่อ	คำเต็ม
AAA	Authentication, Authorization and Accounting
ACL	Access Control List
AES	Advanced Encryption Standard
AP	Access Point
API	Application Programming Interface
APT	Advanced Persistent Threat
ARP	Address Resolution Protocol
AS2	Applicability Statement 2
BeEF	Browser Exploitation Framework
BLE	Bluetooth Low Energy
BSSID	Basic Service Set Identifiers
CA	Certificate Authority
CAPEC	Common Attack Pattern Enumeration and Classification
CLI	Command-Line Interface
CSRF	Cross-Site Request Forgery
CSV	Comma-Separated Values
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring Systems
CWE	Common Weakness Enumeration
DB	Database
DDoS	Distributed Denial-of-Service
DHCP	Dynamic Host Configuration Protocol
DLL	Dynamic Link Library
DLP	Data Loss Prevention
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
EAP	Extensible Authentication Protocol
FOCA	Fingerprinting Organization with Collected Archives
FTP	File Transfer Protocol
FTPS	File Transfer Protocol Secure
GDB	GNU Debugger
GDPR	General Data Protection Regulation
GPU	Graphics Processing Unit
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
ICMP	Internet Control Message Protocol
ICS	Industrial Control System
IDA	Interactive Disassembler
IDS	Intrusion Detection System
IIoT	Industrial Internet of Things
IMEIs	International Mobile Equipment Identity
IoT	Internet of Things
IP	Internet Protocol
IPMI	Intelligent Platform Management Interface
IPS	Intrusion Prevention System
ISO	International Organization for Standardization
ISP	Internet Service Provider
ISSAF	Information Systems Security Assessment Framework
JSON	JavaScript Object Notation
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LLMNR	Link-Local Multicast Name Resolution
LSASS	Local Security Authority Subsystem Service
MAC	Media Access Control
MDM	Mobile Device Management
MobSF	Mobile Security Framework
MOU	Memorandum of Understanding
MSA	Master Service Agreement
MX	Mail Exchange
NAC	Network Access Control
NBT-NS	NetBIOS Name Service
NDA	Non-disclosure Agreement
NFC	Near-Field Communication
NIST	National Institute of Standards and Technology
NIST SP	National Institute of Standards and Technology Special Publication
NS	Name Server
NSE	Nmap Scripting Engine
NTLM	New Technology LAN Manager
NTP	Network Time Protocol
OS	Operating System
OSINT	Open-source Intelligence
OSSTMM	Open-source Security Testing Methodology Manual
OWASP	Open Web Application Security Project
PBKDF2	Password-Based Key Deviation Function 2
PCI DSS	Payment Card Industry Data Security Standard
PHP	PHP: Hypertext Preprocessor
PII	Personal Identifiable Information
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PS	PowerShell
PSK	Pre-Shared Key
PTES	Penetration Testing Execution Standard
RAT	Remote Access Trojan
RDP	Remote Desktop Protocol
RF	Radio Frequency

คำย่อ	คำเต็ม
RFC	Request for Comment
RFID	Radio-Frequency Identification
ROE	Rules of Engagement
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Protocol
SDK	Software Development Kit
SDLC	Software Development Life Cycle
SDR	Software-defined Radio
SET	Social Engineering Toolkit
SGID	Set Group ID
SIEM	Security Information and Event Management
SIP	Session Initiation Protocol
SLA	Service-level Agreement
SMB	Server Message Block
S/MIME	Secure/Multipurpose Internet Mail Extensions
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOC	Security Operations Center
SOW	Statement of Work
SQL	Structured Query Language
SSD	Solid-State Drive
SSH	Secure Shell
SSHD	Solid-State Hybrid Drive
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSO	Single Sign-On
SUID	Set User ID
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TTL	Time to Live
TTPs	Tactics, Techniques and Procedures
UDP	User Datagram Protocol
URL	Uniform Resource Locator
URI	Uniform Resource Identifier
USB	Universal Serial Bus
UTF	Unicode Transformation Format
VAS	Vulnerability Assessment Scanner
VLAN	Virtual Local Area Network
VM	Virtual Machine
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VPS	Virtual Private Server
WAF	Web Application Firewall
WEP	Wired Equivalent Privacy
WiGLE	Wireless Geographic Logging Engine
WinRM	Windows Remote Management
WMI	Windows Management Instrumentation
WPA	Wi-Fi Protected Access
WPS	Wi-Fi Protected Setup
XML-RPC	Extensible Markup Language-Remote Procedure Call
XSS	Cross-Site Scripting
ZAP	Zed Attack Proxy

รายการฮาร์ดแวร์และซอฟต์แวร์ที่มีการเสนอสำหรับข้อสอบ PenTest+

CompTIA แนบตัวอย่างรายการฮาร์ดแวร์และซอฟต์แวร์มาในที่นี้เพื่อช่วยเหลือผู้สมัครสอบในการเตรียมตัวสอบ PenTest+ รายการนี้อาจมีประโยชน์ต่อบริษัทฝึกอบรมที่ต้องการสร้างองค์ประกอบห้องปฏิบัติการสำหรับจัดการฝึกอบรม รายการย่อยในแต่ละหัวข้อเป็นเพียงตัวอย่างโดยคร่าวเท่านั้น

อุปกรณ์

- แล็ปท็อป
- อุปกรณ์กระจายสัญญาณแบบไร้สาย
- เซิร์ฟเวอร์
- Graphics processing unit (GPU)
- สวิตช์
- สายสัญญาณ
- จอภาพ
- ไฟร์วอลล์
- HID/Door access control
- อะแดปเตอร์ไร้สายที่สามารถทำ Packet Injection ได้
- เสาอากาศแบบทิศทาง
- อุปกรณ์เคลื่อนที่
- อุปกรณ์ IoT (กล้อง, Raspberry Pi, สมาร์ททีวี ฯลฯ)
- อะแดปเตอร์บลูทูธ
- การเข้าถึงสภาพแวดล้อมระบบคลาวด์
  - การเข้าถึง Command-Line Interface (CLI)
  - การเข้าถึงคอนโซลการจัดการ
  - อินสแตนซ์ของบริการคลาวด์
- เครื่องพิมพ์เอนกประสงค์ (ใช้สาย/ไร้สาย)
- เครื่องพิมพ์ร่วมโดเมน
- ตัวอ่าน RFID
- อุปกรณ์ตรวจสอบทางชีวภาพ
- Programmable Logic Controller
  - ชุด Software-Defined Radio (SDR)
- แฟลชไดรฟ์ USB
  - USB ไดรฟ์ติดอาวุธ

ฮาร์ดแวร์สำรอง

- เคเบิล
- แป้นพิมพ์
- เมาส์
- แหล่งจ่ายไฟ
- ดองเกิล/อะแดปเตอร์

อะไหล่สำรอง

- เคเบิล HDMI
- ฮาร์ดไดรฟ์สำรอง
- จอภาพสำรอง

เครื่องมือ

- ชุดงัดกุญแจ
- ตัวโคลนป้ายชื่อ
- ตัวเก็บรอยนิ้วมือ
- ยาทาเล็บ (เพื่อปกปิดรอยนิ้วมือ)

ซอฟต์แวร์

- สิทธิ์การใช้งาน OS
- OS แบบโอเพ่นซอร์ส
- กรอบงานทดสอบเจาะระบบ
- ซอฟต์แวร์ VM
- เครื่องมือสแกน
- เครื่องมือทดสอบข้อมูลประจำตัว
  - เครื่องมือ Spraying
  - โปรแกรมเจาะรหัสผ่าน
- เครื่องมือแก้จุดบกพร่อง
- เครื่องมือทดสอบเพื่อหาบั๊ก
- เครื่องมือประกันซอฟต์แวร์
- เครื่องมือทดสอบไร้สาย
- เครื่องมือพร็อกซี่เว็บ
- เครื่องมือวิศวกรรมสังคม
- เครื่องมือการเข้าถึงระยะไกล
- เครื่องมือเครือข่าย
- เครื่องมือทดสอบการเคลื่อนไหว
- ข้อมูลการรักษาความปลอดภัยและการ จัดการกิจกรรม (SIEM)/ระบบ ตรวจจับการบุกรุก (IDS)/ ระบบ ป้องกันการบุกรุก (IPS)
- เครื่องมือบัญชาการและควบคุม
- เครื่องมือตรวจจับและหลีกเลี่ยง