**Final Quiz Penetration Testing (30 คะแนน)**

1. จงเขียนอธิบายขั้นตอนในการโจมตีตามหลักของ Cyber Kill Chain (3 คะแนน)

* Recon -> ทำความรู้จักเป้าหมาย
* Weaponization -> เลือกเครื่องมือ / Payload ที่จะใช้โจมตี
* Delivery -> เลือกวิธีส่ง Payload
* Exploit -> เริ่ม Payload ให้โจมตี
* Install -> ฝัง Backdoor
* Command and Control -> สื่อสารและควบคุมเครื่องเหยื่อเพื่อใช้ประโยชน์
* Action on Objective -> ขโมยข้อมูล / ทำลาย / หรือให้ Attack เครื่องอื่นต่อ

1. การรวบรวมข้อมูลเป้าหมายเบื้องต้น : จงรวบรวมข้อมูลดังต่อไปนี้ โดยอาศัยการ Google Dorkling พร้อมระบุ Keyword ที่ใช้ในการสืบค้น และ Passive Scan ระบุวิธีทำด้วย (10 คะแนน)

Keyword : site:\*.psu.ac.th -inurl:https inurl:php

* ระบุอย่างน้อย 1 เว็บไซต์ภายในโดเมน หรือ ซับโดเมนของ psu.ac.th ที่พัฒนาโดยเทคโนโลยีเก่า หรือไม่ได้อัพเดทเว็บไซต์มานานแล้ว

<https://tracking.surat.psu.ac.th/it/pdffile/print.php?id=8253>

<https://tracking.surat.psu.ac.th>

* สืบหาคณะ / หน่วยงานผู้รับผิดชอบเว็บดังกล่าว

ศูนย์สนเทศและการเรียนรู้ มอ.สุราษฎร์

* ในหน่วยงานผู้รับผิดชอบดังกล่าวนั้น ผู้รับผิดชอบ หรือ ผู้ติดต่อประสานงานเว็บนี้คือใครง

เนาวรัตน์ บุญนวล

* เว็บนี้สร้างโดยเทคโนโลยีใด อยู่บน Server แบบใด

PHP : Unknown version, Apache HTTPD server : Unknown version

* Server นี้มี CVE หรือไม่

ไม่ทราบ เนื่องจาก Server ไม่ได้ Response Version กลับมา จึงทำให้ไม่สามรถสืบค้นเบอร์ CVE ต่อได้

1. กำหนดเป้าหมาย IP 172.28.48.249:8080

จงดำเนินการ Penetration Testing ให้เสร็จสมบูรณ์พร้อมเขียนรีพอร์ตที่มีข้อมูลดังนี้

* IP เป้าหมาย, พอร์ตที่เปิด, เครื่องมือที่ใช้ในการทดสอบ (1 คะแนน)

IP : 172.28.48.249

Opened ports :

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds?

902/tcp open ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)

912/tcp open vmware-auth VMware Authentication Daemon 1.0 (Uses VNC, SOAP)

2179/tcp open vmrdp?

8080/tcp open http Apache httpd 2.4.54 ((Debian))

Tool : Zenmap + Nmap (nmap -sS -sV -T4 -A -v 172.28.48.249)

* ผลการทดสอบ (แต่ละรูรั่วให้รายงานผลดังนี้)
  + รูรั่วที่พบ (ระบุรูรั่วที่พบ) 1 คะแนน
    - Joomla 4.0.0 – 4.2.7 Unauthorized Access Vulnerability

CVE-2023-23752 (at http://172.28.48.249:8080/api/index.php/v1/config/application?public=true)

* + ผลกระทบที่เกิดขึ้น 1 คะแนน
    - ได้ user / password ของ db โดยไม่รับอนุญาต ซึ่งอาจนำไปสู่การขโมยข้อมูล
  + วิธีป้องกัน 1 คะแนน
    - Update Joomla CMS ไป Version ล่าสุด (Joomla >=4.2.8)
  + หลักฐานการทดสอบรูรั่ว (หลักฐานว่า Hack ได้แล้วจริง) 2 คะแนน
    - รูปภาพประกอบด้วย ข้อความ, ภาพหน้าจอ, ซอฟต์แวร์, ซอฟต์แวร์มัลติมีเดีย

      เนื้อหาที่สร้างโดย AI อาจไม่ถูกต้อง
    - รูปภาพประกอบด้วย ข้อความ, อิเล็กทรอนิกส์, ภาพหน้าจอ, ซอฟต์แวร์

      เนื้อหาที่สร้างโดย AI อาจไม่ถูกต้อง

1. กำหนดเป้าหมาย IP 172.28.48.243

จงดำเนินการ Penetration Testing ให้เสร็จสมบูรณ์พร้อมเขียนรีพอร์ตที่มีข้อมูลดังนี้

* IP เป้าหมาย, พอร์ตที่เปิด, เครื่องมือที่ใช้ในการทดสอบ (1 คะแนน)

IP : 172.28.48.243

Opened ports:

21/tcp open ftp ProFTPD 1.3.5

22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)

80/tcp open http Apache httpd 2.4.7

445/tcp open netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)

631/tcp open ipp CUPS 1.7

3000/tcp closed ppp

3306/tcp open mysql MySQL (unauthorized)

8080/tcp open http Jetty 8.1.7.v20120910

Tool : Zenmap + Nmap (nmap -sS -sV -T4 -A -v 172.28.48.243)

* ผลการทดสอบ (รายงาน 2 รูรั่ว : แต่ละรูรั่วให้รายงานผลดังนี้)

รูรั่ว 1

* + รูรั่วที่พบ (ระบุรูรั่วที่พบ) 2 คะแนน
    - ProFTPD 1.3.5 RCE via mod\_copy (CVE-2015-3306)
  + ผลกระทบที่เกิดขึ้น 2 คะแนน
    - สามารถรันโค้ดในเครื่องเป้าหมายโดยไม่ได้รับอนุญาต ซึ่งอาจนำไปสู่การขโมยข้อมูล
  + วิธีป้องกัน 2 คะแนน
    - Update ProFTPD ไปเป็นเวอร์ชั่นล่าสุด หรือ Block ProFTPD ให้เข้าได้จาก Network ที่น่าเชื่อถือเท่านั้น
  + หลักฐานการทดสอบรูรั่ว (หลักฐานว่า Hack ได้แล้วจริง) 4 คะแนน

รูปภาพประกอบด้วย ข้อความ, ภาพหน้าจอ, ตัวอักษร

เนื้อหาที่สร้างโดย AI อาจไม่ถูกต้อง

รูปภาพประกอบด้วย ข้อความ, ภาพหน้าจอ, ตัวอักษร

เนื้อหาที่สร้างโดย AI อาจไม่ถูกต้อง

รูรั่ว 2

* + รูรั่วที่พบ (ระบุรูรั่วที่พบ) 2 คะแนน
    - XSS (at http://172.28.48.243/chat/)
    - Payload : <script>

window.name = 'https://www.youtube.com/watch?v=Hqssy5jna\_U';

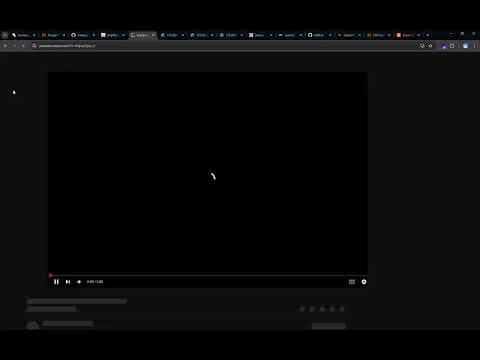
function blah() {}

blah("" + new class b {

toString = e => location = name;

} + "")

</script>

* + ผลกระทบที่เกิดขึ้น 2 คะแนน
    - ฝัง JavaScript ลงไปในช่องข้อความของ ChatRoom ได้ ทำให้ทุกครั้งที่เรียกใช้ ChatRoom, Script ที่ฝังไว้จะ Run ทันที อาจจะทำให้ขโมย Cookies, Session ออกไปได้
  + วิธีป้องกัน 2 คะแนน
    - Validate User Input ทุกครั้ง
  + หลักฐานการทดสอบรูรั่ว (หลักฐานว่า Hack ได้แล้วจริง) 4 คะแนน
    - <https://youtu.be/wvXqurRb3N8>
    - [](https://www.youtube.com/embed/wvXqurRb3N8?feature=oembed)