กรอบแนวทางในการดำเนินการ จัดทำ Penetration Testing เบื้องต้นสำหรับผู้ดูแลระบบ

Penetration Test เป็นกระบวนการทดสอบและจำลองเหตุการณ์ hack ระบบสารสนเทศ โดยใช้กลยุทธ์และเครื่องมือที่เหมาะสมเพื่อเจาะเข้าสู่ระบบ ซึ่งจะช่วยให้ทราบจุดแข็งและจุดอ่อนของระบบ ทั้งนี้ระบบสารสนเทศ จะต้องมีการบริหารจัดการด้านความปลอดภัยของข้อมูล เพื่อทำให้เกิดความปลอดภัยของข้อมูล ได้แก่

1. การจัดการด้านความปลอดภัยของเครื่องคอมพิวเตอร์แม่ข่ายและระบบสารสนเทศ
   (1) การออกแบบระบบให้มีความปลอดภัย
   (2) การ update patch ระบบปฏิบัติการ
   (3) การติดตั้ง Software Antivirus
   (4) การตั้งค่า firewall บนเครื่องแม่ข่าย
   (5) การเข้ารหัสข้อมูลด้วยวิธีการต่าง ๆ เช่น วิธีรการ hash ข้อมูล, การใช้ช่องทาง ssl
   (6) การจัดการด้านสิทธิ์ของผู้ใช้งานระบบ
   (7) การ backup สำรองขอมูล

2. การป้องกันความปลอดภัยด้านระบบเครือข่าย
   (1) การใช้งานอุปกรณ์ป้องกันความปลอดภัยของระบบเครือข่าย (firewall) , IDS/IPS การตรวจจับผู้บุกรุก
   (2) การควบคุม Network Zone ต่างๆ
   (3) การจัดการด้านสถาปัตยกรรมเครือข่าย
   (4) การจัดการการเข้าถึงระบบเครือข่าย ระบบคอมพิวเตอร์ต่างๆ
   (5) การใช้งานโพรโทคอลต่างๆ
   (6) การจัดการความปลอดภัยทางด้าน physical control

ขั้นตอนจัดทำ Penetration Test ประกอบด้วย 5 ขั้นตอน ดังนี้

1. การวางแผนและการสำรวจ

เป็นขั้นตอนแรกเกี่ยวข้องกับการวางแผนเพื่อจัดเตรียมการโจมตี โดยเป็นการสำรวจรวบรวมข้อมูลในระบบให้ได้มากที่สุด อาจเป็นขั้นตอนที่ใช้เวลานานที่สุด ซึ่งมีกระบวนการตรวจสอบระบบ สังเกตช่องโหว่ และวิธีที่องค์กรตอบสนองต่อการละเมิดระบบ โดยข้อมูลที่ค้นหามีตั้งแต่ชื่อและที่อยู่อีเมลของพนักงานของบริษัท ไปจนถึง topology ของระบบเครือข่าย ที่อยู่ IP และอื่นๆ สังเกตได้ว่าประเภทของข้อมูลหรือระดับความลึกของการตรวจสอบจะขึ้นอยู่กับวัตถุประสงค์ที่กำหนดไว้สำหรับการตรวจสอบ วิธีการรวบรวมข้อมูลเช่น social engineering, dumpster diving, network scanning, domain registration information เป็นต้น

2. การสแกนระบบ

จากขั้นตอนการวางแผนและสำรวจ ผู้ทดสอบการเจาะระบบจะใช้เครื่องมือสแกนเพื่อสำรวจจุดอ่อนของระบบและเครือข่าย โดยการสแกนระบบนี้ จะพบจุดอ่อนของระบบ ที่อาจใช้สำหรับการโจมตีได้
ตัวอย่างเช่น ระบบสารสนเทศ : Web Application
มาตราฐานความปลอดภัย : OWASP (จัดทำขึ้นโดยองค์กรไม่แสวงหาผลกำไร)
เครื่องมือ : WEBGOAT, DVWA, SQLi-Labs เพื่อสแกนหาจุดอ่อนของระบบ

3. การเข้าถึงระบบ

เมื่อเข้าใจถึงช่องโหว่ของระบบแล้ว ผู้ทดสอบการเจาะระบบจะพยายามเจาะเข้าระบบโดยใช้ประโยชน์จากจุดอ่อนด้านความปลอดภัย ซึ่งผู้ทดสอบการเจาะระบบจะพยายามเปลี่ยนแปลงสิทธิ์บนระบบ เพื่อแสดงให้เห็นว่าผู้ทดสอบการเจาะระบบจะสามารถเข้าไปในสภาพแวดล้อมเชิงลึกของระบบได้อย่างไร

4. การเข้าถึงแบบถาวร

ขั้นตอนนี้เป็นการใช้ประโยชน์จากช่องโหว่จากสิทธิ์การเข้าถึง เมื่อผู้ทดสอบการเจาะระบบตั้งหลักในระบบแล้ว ผู้ทดสอบการเจาะระบบจะรักษาการเข้าถึงและควบคุมการโจมตีที่จำลองไว้นานพอที่จะบรรลุผลสำเร็จและทำซ้ำเป้าหมายของแฮ็กเกอร์ที่เป็นอันตราย ดังนั้นในระยะนี้ผู้ทดสอบการเจาะระบบจึงพยายามรับระดับสิทธิ์สูงสุดในระบบ

5. การวิเคราะห์/รายงานขั้นสุดท้าย

เป็นการรายงานผลมาจากการทดสอบการเจาะ ในขั้นตอนสุดท้าย ทีมรักษาความปลอดภัยจะเตรียมรายงานโดยละเอียดซึ่งอธิบายขั้นตอนการทดสอบการเจาะระบบทั้งหมด ข้อมูลหรือ รายละเอียดบางอย่างที่ควรปรากฏ ได้แก่

(1) ความร้ายแรงของความเสี่ยงที่เกิดจากช่องโหว่ที่ค้นพบ
(2) เครื่องมือที่สามารถเจาะระบบได้สำเร็จ
(3) เน้นย้ำจุดที่มีการรักษาความปลอดภัยอย่างถูกต้อง
(4) ช่องโหว่เหล่านั้นที่ต้องแก้ไขและวิธีป้องกันการโจมตีในอนาคต (คำแนะนำการแก้ไข)

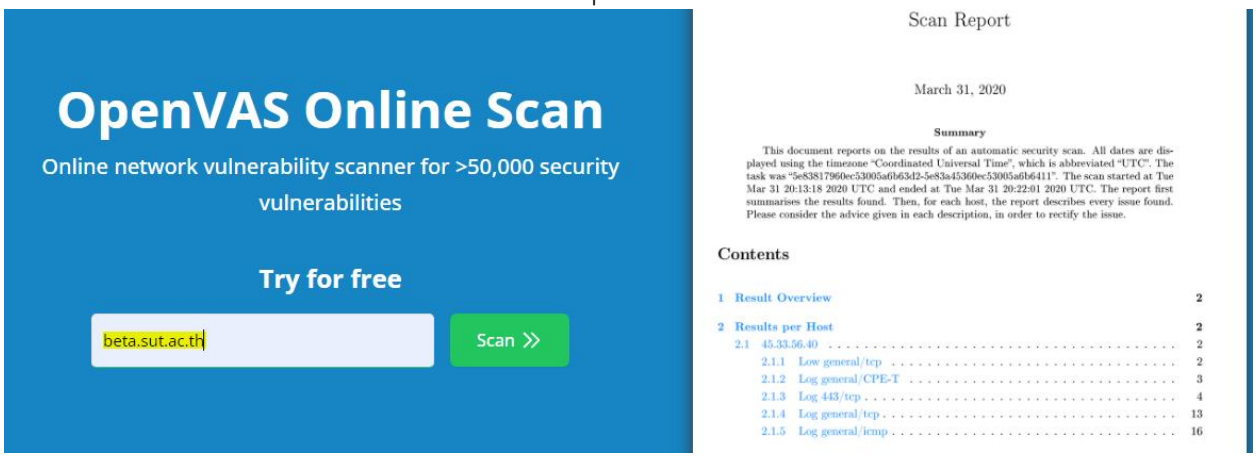
ขั้นตอนนี้อาจมีความสำคัญที่สุดสำหรับทั้งสองฝ่าย เนื่องจากเจ้าหน้าที่ไอทีและผู้จัดการที่ไม่ใช่ฝ่ายเทคนิคมักอ่านรายงานนี้ จึงแนะนำให้แยกรายงานออกเป็นส่วนคำอธิบายทั่วไปและด้านเทคนิคเพิ่มเติม เช่น รายงานผู้บริหารและรายงานทางเทคนิค

- **แนะนำเครื่องมือในการสแกนระบบแบบออนไลน์**

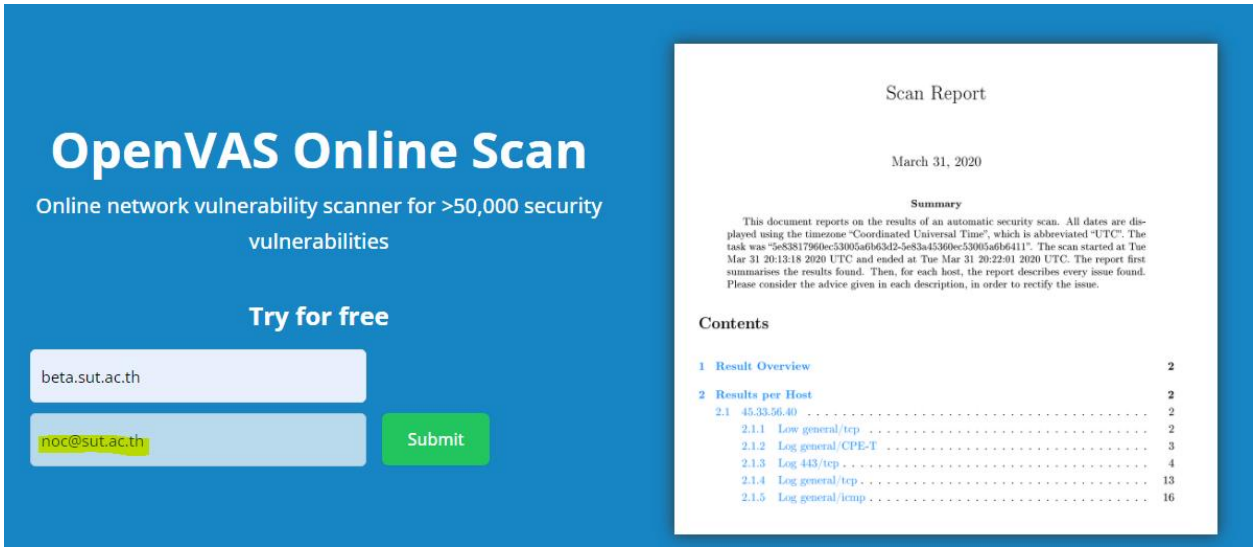
เว็บไซต์ OpenVas Online Scan (https://hostedscan.com/openvas-vulnerability-scan)
ข้อดี จะมีวิธีการประมวลผลหลายวิธี จากการ submit url เพียงครั้งเดียว
ข้อเสีย เป็นการบอกจุดอ่อนคร่าวๆ ไม่ได้ลงลึกถึง detail มากนัก
นอกจากนี้ยังมีเว็บไซต์อื่นๆ เช่น https://sitecheck.sucuri.net/ และ https://pentest-tools.com/website-vulnerability-scanning/website-scanner

- **วิธีการใช้งาน** (OpenVas Online Scan)

1. กรอก url ระบบสารสนเทศ หรือ หมายเลข ip address ที่ต้องการแสกนลงในเว็บไซต์

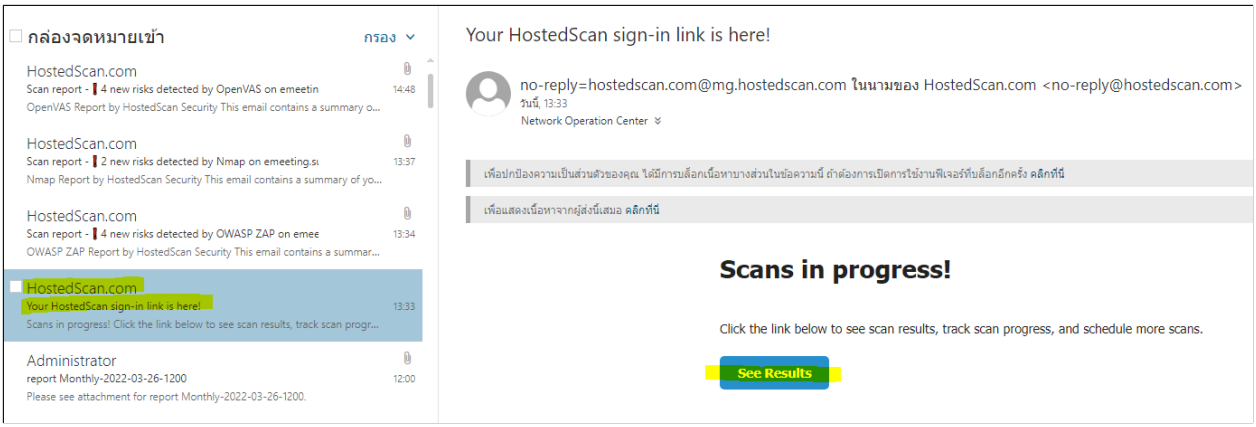


2. กรอก email address เพื่อรับผลการสแกน และกด submit เพื่อรับผลการตรวจสอบเว็บไซต์



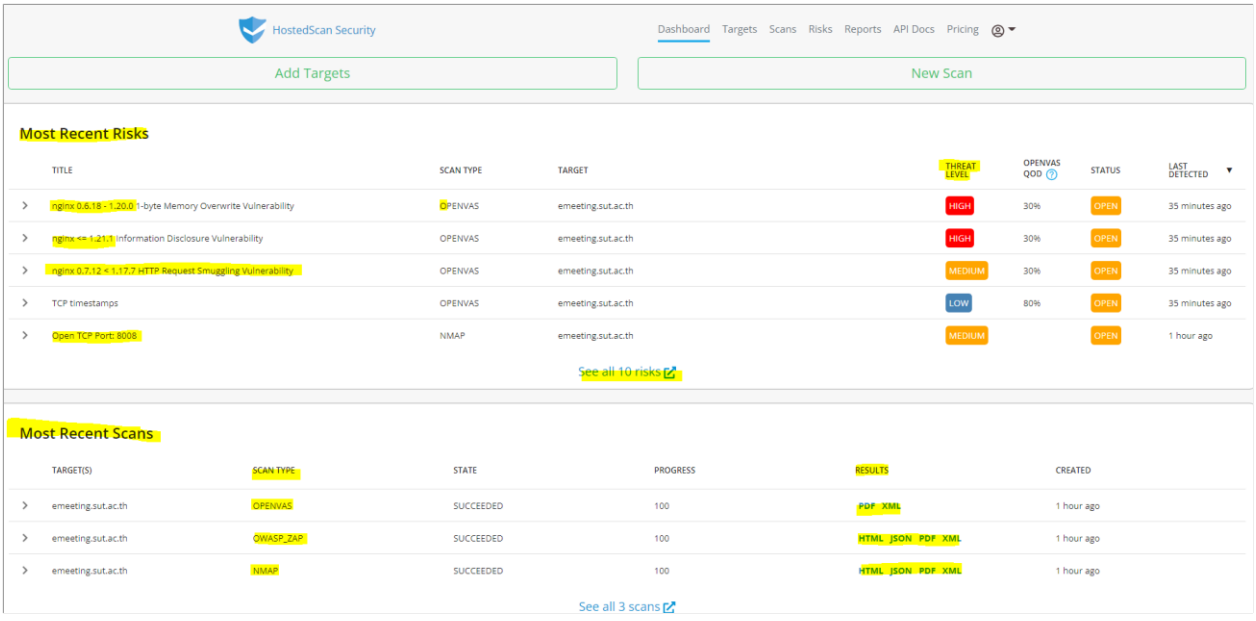
- **การวิเคราะห์ผล**

1.ภายหลังการ sumbit url หรือ ip เข้าระบบสแกนออนไลน์ ระบบจะทำการแจ้งผลโดยส่งข้อมูลเข้า email ที่เราได้ให้ไว้ ซึ่งสามารถดูรายละเอียดการสแกนได้ดังตัวอย่างต่อไปนี้



รูปภาพแสดงการแจ้งผลมาที่ email

2. เมื่อได้รับ email คลิ้กที่ see results เพื่อทราบผลการสแกน



3. ที่หัวข้อ Most Recent Risks ระบบแจ้งจุดอ่อนของระบบสารสนเทศ (อาจเลือกให้แสดงผลแบบ 10 อันดับเพื่อทราบจุดอ่อนอื่น ๆ โดยสามารถคลิกเลือกได้จากเมนู “See all 10 risks”)

Risks

	TITLE	SCAN TYPE	TARGET	THREAT LEVEL
>	nginx 0.6.18 - 1.20.0 1-byte Memory Overwrite Vulnerability	OPENVAS	emeeting.sut.ac.th	HIGH
>	nginx <= 1.21.1 Information Disclosure Vulnerability	OPENVAS	emeeting.sut.ac.th	HIGH
>	nginx 0.7.12 < 1.17.7 HTTP Request Smuggling Vulnerability	OPENVAS	emeeting.sut.ac.th	MEDIUM
>	TCP timestamps	OPENVAS	emeeting.sut.ac.th	LOW
>	Open TCP Port: 8008	NMAP	emeeting.sut.ac.th	MEDIUM
>	Open TCP Port: 80	NMAP	emeeting.sut.ac.th	MEDIUM
>	Application Error Disclosure	OWASP_ZAP	emeeting.sut.ac.th	MEDIUM
>	X-Frame-Options Header Not Set	OWASP_ZAP	emeeting.sut.ac.th	MEDIUM
>	Information Disclosure - Debug Error Messages	OWASP_ZAP	emeeting.sut.ac.th	LOW
>	X-Content-Type-Options Header Missing	OWASP_ZAP	emeeting.sut.ac.th	LOW

- **ตัวอย่างการแปลผล**
  - nginx ซึ่งเป็น web server ของระบบ outdate อาจทำให้เกิด memory overwrite ซึ่งเป็น threat ระดับ High ควรแก้ไขโดยด่วน
  - มีการเปิด port 8008 ซึ่งเป็น threat ระดับ medium ผู้ดูแลระบบสารสนเทศอาจดำเนินการปิด port ของเครื่องแม่ข่ายได้ หากไม่ได้มีการใช้งานผ่าน port ดังกล่าว เป็นต้น
  - ไม่มีการ set ค่า x-frame-option header ซึ่งการตั้งค่าดังกล่าว จะสามารถป้องการวิธีการ 'ClickJacking' attacks. ได้

ทั้งสามารถเลือกเมนู > เพื่อสามารถทราบรายละเอียดเพิ่มเติมได้

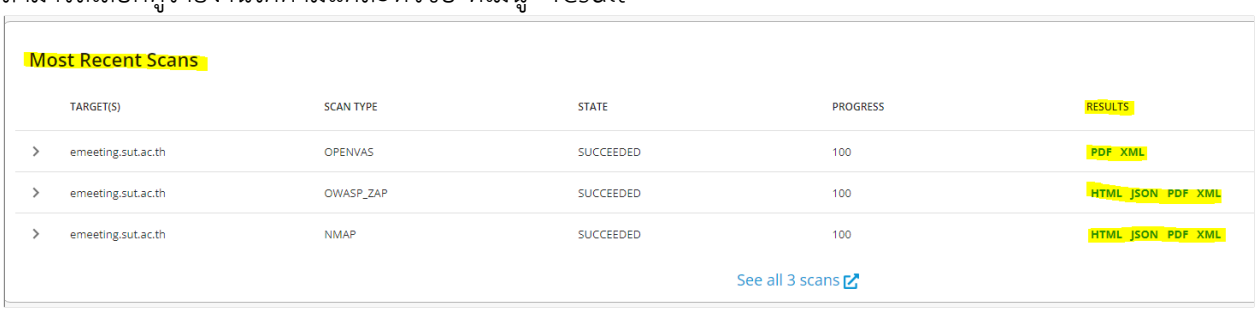
X-Frame-Options Header Not Set OWASP_ZAP emeeting.sut.ac.th

Name	X-Frame-Options Header Not Set
Description	X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.
Solution	Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. A
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
CWE Id	1021
WASC Id	15
Other Information	
Instances	uri: http://emeeting.sut.ac.th method: GET param: X-Frame-Options attack: evidence:

4. ที่หัวข้อ Most Recent Risks ระบบได้ทำการสแกนระบบสารสนเทศ โดยวิธีการอื่น ๆ และสามารถออก report ตามแต่ละประเภทเครื่องมือ เพื่อทราบรายละเอียดหรือวิธีการแก้ไขจุดอ่อนของระบบเพิ่มเติม ได้แก่

- รูปแบบการสแกนแบบ Openvas
- รูปแบบการสแกนแบบ OWASP_ZAP
- รูปแบบการสแกนแบบ NMAP

สามารถเลือกดูรายงานได้ตามแต่ละหัวข้อ ที่เมนู “result”



ตัวอย่างการออก report

Scan Report

March 26, 2022

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone “Coordinated Universal Time”, which is abbreviated “UTC”. The task was “623eb39b5eb6840040dfbf15-623eb39d5eb6840040dfbf1d”. The scan started at Sat Mar 26 06:33:41 2022 UTC and ended at Sat Mar 26 07:47:35 2022 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

2.1.1 High 80/tcp

แจ้งจุดอ่อนที่พบ

High (CVSS: 9.4)
NVT: nginx 0.6.18 - 1.20.0 1-byte Memory Overwrite Vulnerability

Product detection result
cpe:/a:f5:nginx:1.16.1
Detected by nginx Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.113787)

Summary
...continues on next page ...

...continued from previous page ...

nginx is prone to a 1-byte memory overwrite vulnerability.

Vulnerability Detection Result

แจ้งจุดอ่อนที่พบ

Installed version: 1.16.1
Fixed version: 1.20.1/1.21.0
Installation
path / port: 80/tcp

Solution:

แจ้ง solution การแก้ไขปัญหา

Solution type: VendorFix
Update to version 1.20.1, 1.21.0 or later.

Affected Software/OS

nginx version 0.6.18 through 1.20.0.
Note: The issue only affects nginx if the 'resolver' directive is used in the configuration file. Further, the attack is only possible if an attacker is able to forge UDP packets from the DNS server.

Vulnerability Insight

A security issue in nginx resolver was identified, which might allow an attacker to cause 1-byte memory overwrite by using a specially crafted DNS response, resulting in worker process crash or, potentially, in arbitrary code execution.

- **ข้อแนะนำ**

  นอกจากการดำเนินการแก้ไขจุดอ่อนของระบบสารสนเทศ ตามที่ได้รับทราบแล้ว ระบบสารสนเทศที่มีการให้บริการในรูปแบบเว็บไซต์ ควรจัดให้มีการใช้งานผ่านช่องทาง SSL ช่วยเพิ่มความปลอดภัยในการสื่อสารข้อมูลบนเครือข่ายอินเตอร์เน็ต เนื่องจาก SSL ทำการเข้ารหัสข้อมูลระหว่างผู้ใช้กับเซิร์ฟเวอร์ ช่วยป้องกันการถูกดักจับหรือเปิดอ่านข้อมูลระหว่างทาง (sniffing) ได้ทั้งนี้ ท่านสามารถขอใช้งาน SSL certificate ได้ฟรี จากบริการของศูนย์คอมพิวเตอร์ สามารถดูรายละเอียดเพิ่มเติมได้ที่ http://its.sut.ac.th/index.php?option=com_content&view=article&id=55